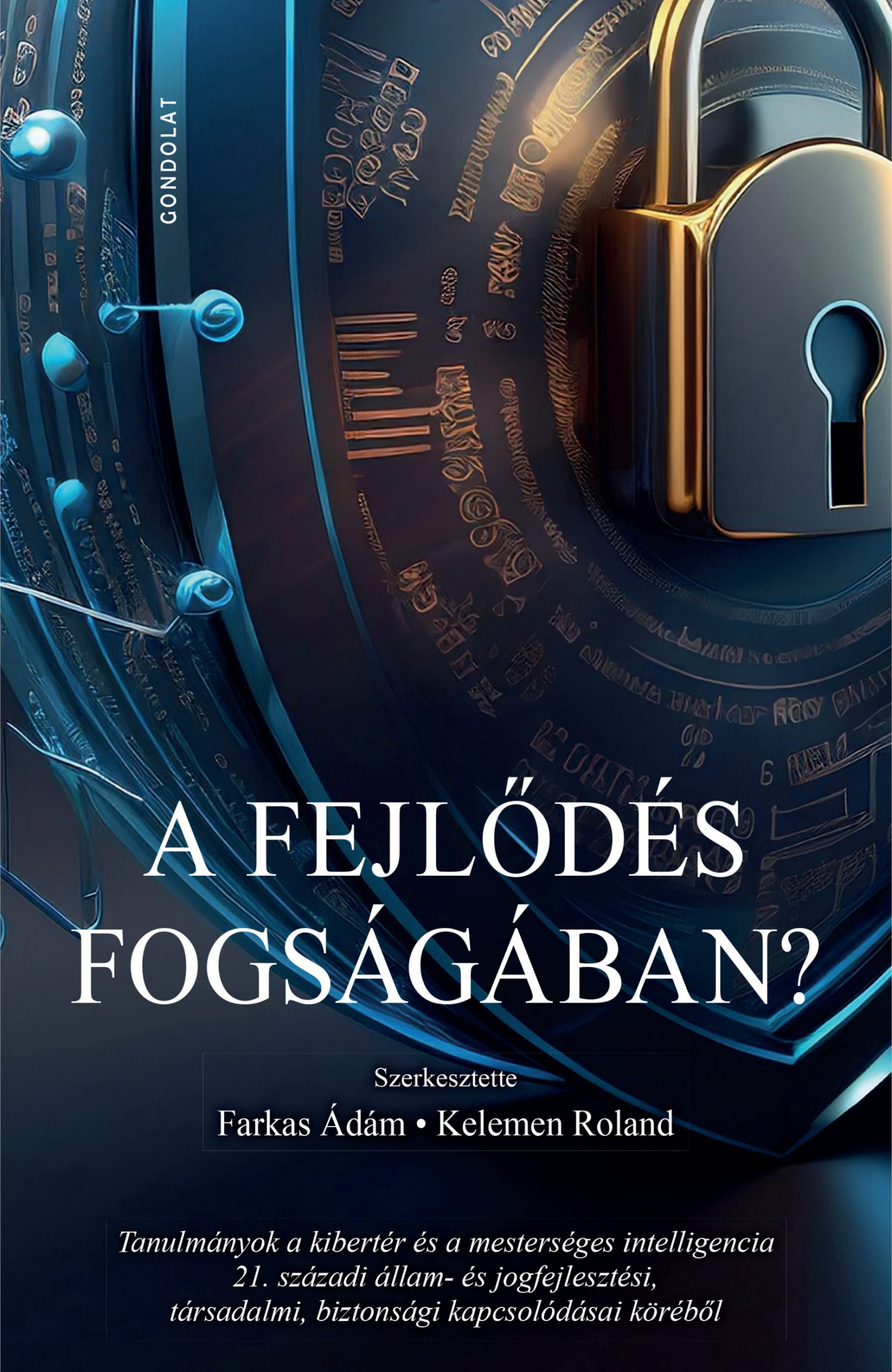


A FEJLŐDÉS FOGSÁGÁBAN?

Szerkesztette
Farkas Ádám • Kelemen Roland

Tanulmányok a kibertér és a mesterséges intelligencia 21. századi állam- és jogfejlesztési, társadalmi, biztonsági kapcsolódásai köréből

A FEJLŐDÉS FOGSÁGÁBAN?

A FEJLŐDÉS FOGSÁGÁBAN?

Tanulmányok a kibertér és a mesterséges intelligencia 21. századi állam- és jogfejlesztési, társadalmi, biztonsági kapcsolódásai köréből

Szerkesztette
Farkas Ádám • Kelemen Roland

Gondolat Kiadó
Budapest, 2023

A TKP2021-NVA-24 azonosítószámú projekt a Kulturális
és Innovációs Minisztérium Nemzeti Kutatási Fejlesztési
és Innovációs Alapból nyújtott támogatásával,
a Tématerületi Kiválósági Program 2021 – Nemzetvédelem, nemzetbiztonság
pályázati alprogram finanszírozásában valósult meg.



AZ NKFI ALAPBÓL
MEGVALÓSULÓ
PROGRAM

SZERZŐK
Bányász Péter • Bartkó Róbert • Deli Gergely • Farkas Ádám •
Gál István László • Gosztonyi Gergely • Hódos László • Kádár Pál • Kassai Károly
• Kelemen Roland • Krasznay Csaba • Pongrácz Alex • Simon László •
Smuk Péter • Spitzer Jenő • Tóth András • Vikman László

A kéziratok 2022. december 15-én kerültek lezárásra.

© Szerzők, 2023
Szerkesztés © Farkas Ádám, Kelemen Roland, 2023

Minden jog fenntartva. Bármilyen másolás, sokszorosítás, illetve adatfeldolgozó
rendszerben való tárolás a kiadó írásbeli hozzájárulásához van kötve.

www.gondolatkiado.hu
facebook.com/gondolat

A kiadásért felel Bácskai István
Tördelés Lipót Éva

ISBN 978 963 556 480 4

Tartalom

Előszó 9

Kelemen Roland

Cyberfare State modelljei. A digitális állam lehetséges irányai 13
1. A kibertér államra gyakorolt hatása 14
2. Cyberfare State modelljei 29

Pongrácz Alex

Gondolatok a kibertér és a digitalizáció állammodellkérdésre gyakorolt hatásairól 43

Simon László

Az egyén mint nem állami szereplő a kibertérben megjelenő fenyegetési palettán, avagy a kiberpartizán kérdése 55
1. A világrend biztonsági hálója a biztonságos hálózatok világrendje 56
2. Az egyén/felhasználó mint nem állami hatalmi szereplő az információs társadalomban 61
3. Az információ mint a fenyegetés eszköze 65
4. A fegyveres konfliktust támogató hacktivista: a kiberpartizán 71

Farkas Ádám

A kibertér műveleti tevékenységek egyes szabályozási és államszervezési alapkérdései 77
1. A szakmai követelmények, a nemzetközi jog és a nemzetállami szabályozás háromszögében 80
2. A jó kormányzás, a komplex biztonság és a megalapozott döntéshozatal igényeinek kapcsolata a kibertérműveleti képességekkel 87

Vikman László

GONDOLATOK A KIBERBIZTONSÁGI STRATÉGIÁK FEJLESZTÉSÉRE VONATKOZÓ NEMZETKÖZI ÚTMUTATÓ KAPCSÁN 97
1. Az NCS Guide – Útmutató egy nemzeti kiberbiztonsági stratégia kidolgozásához 99
2. Észrevételek és gondolatok az útmutató kapcsán 103

Deli Gergely

AZ ATOMHÁBORÚ ESÉLYEI A MESTERSÉGES INTELLIGENCIA KORÁBAN 107
1. Az MI szerepe a háború és béke kérdésében 108
2. A liberális békeelméletek intézményi és egyéni előfeltételei 110
3. Gépi kontra emberi „világmegértés" 111

Smuk Péter

A POLITIKAI DISKURZUS ÉS TORZULÁSAI: SZABAD DELIBERÁCIÓ VS. BEFOLYÁSOLÁS 119
1. A politikai diskurzusok demokratikus jelentőségéről és alkotmányos garanciáiról 119
2. A szabad internet romantikája 123
3. A politikai diskurzusok torzulása az online térben – és a lehetséges válaszok 126
4. Konklúzió 133

Gosztonyi Gergely

AZ ÁLLAMOK ÁLTAL VÉGZETT INTERNETKORLÁTOZÁS KÜLÖNBÖZŐ ESZKÖZEI MINT NEMZETBIZTONSÁG ÉS SZÓLÁSSZABADSÁGI KOCKÁZATOK 135
1. Bevezetés 136
2. „A szűrés, a blokkolás és a hekkelés váltotta fel az ollót és a fekete tintát" 137
3. Az internetelérés korlátozása állami eszközökkel Afganisztántól Ukrajnáig 139
4. A 'szilánkos internet' veszélye 145
5. Konklúzió 147

Kádár Pál

A KIBERTÉR ÉS A KIBERTÉRMŰVELETI KÉPESSÉGEK JELENTŐSÉGE A VÉDELMI ÉS BIZTONSÁGI TEVÉKENYSÉGEK ÖSSZEHANGOLÁSÁNAK FEJLESZTÉSÉBEN 149
1. A védelmi és biztonsági szabályozási reform és a kiberműveletek összefüggései 149
2. Az Alaptörvény különleges jogrendi rendelkezései és a kibertér kihívásai 153

3. A védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvény és a kibertér kihívásai 156
4. A honvédelemről és a Magyar Honvédségről szóló 2021. évi CXL. törvény és a kibertér kihívásai 162
5. A koordináció jelentősége 163

Bányász Péter – Krasznay Csaba – Tóth András

A KIBERVÉDELEM SZAKPOLITIKAI SZINTJÉNEK HELYZETE ÉS KIHÍVÁSAI MAGYARORSZÁGON, AZ EU-BAN ÉS A NATO-BAN 167
1. A kibervédelem szakpolitikai szintjének helyzete és kihívásai Magyarországon 168
2. A kibervédelem szakpolitikai szintjének helyzete és kihívásai a NATO-ban 176
3. A kibervédelem szakpolitikai szintjének helyzete és kihívásai az Európai Unióban 184

Kassai Károly

A KIBERTÉRMŰVELETI KÉPESSÉG SZEREPÉNEK, JELENTŐSÉGÉNEK ÉS FÓKUSZÁNAK EVOLÚCIÓJA A NATO STRATÉGIAI DOKUMENTUMAI ALAPJÁN 195
1. A katonai alkalmazás szükségessége a kibertérben – az 1999-es NATO Stratégiai koncepció érvényessége idején 196
2. További lépések az új stratégiai koncepció nyomvonalán 205

Spitzer Jenő – Vikman László

KATONAI ÉS NEMZETBIZTONSÁGI KÉPESSÉGFEJLESZTÉSEK ÉS AZOK JOGI, JOGPOLITIKAI HÁTTERE EGYES TRANSZATLANTI ÁLLAMOKBAN 233
1. Képességfejlesztési törekvések és azok nemzetközi keretei 233
2. Jogi kérdéseket felvető képességfejlesztések egyes transzatlanti államokban 236
3. Várható jövőbeli képességfejlesztési irányok és ezek jogi konzekvenciái 258

Hódos László

A KIBERTÉR ÉS A MESTERSÉGES INTELLIGENCIA JELENTŐSÉGE ÉS KIHÍVÁSAI A JOGÁLLAMOK NEMZETBIZTONSÁGI FELADATELLÁTÁSÁBAN 261
1. A témaválasztás aktualitása, információfúzió, adatanalitika, mesterséges intelligencia 261
2. A proaktív szemléletmód megjelenése a szakmai javaslatok jogi megvalósítása során 264
3. Hibrid hadviselés és kibervédelem 266

4. A mindennapokban megjelenő mesterséges intelligencia és egyes biztonsági aspektusok 267
5. A mesterséges intelligencia a társadalom hibrid fenyegetések, rosszindulatú informatikai tevékenységek és dezinformáció elleni védelmében 272

Gál István – Bartkó Róbert
A KIBERTÉRBEN MEGJELENŐ KIHÍVÁSOK ÉS FENYEGETÉSEK BÜNTETŐJOGI KEZELÉSÉNEK TENDENCIÁI 277
1. Terrorizmus a kibertérben 280
2. A kiberterrorizmus kriminalizálása a hazai büntetőjogban 282
3. Terrorizmus finanszírozása a kibertérben 290

BIBLIOGRÁFIA 303

Előszó

„A kort kell ezért megértenünk, amelybe születtünk. Aki nem érez rá, nem fogja fel legtitkosabb erőit, aki nem érez önmagában valamilyen rokon vonást, mely előrehajtja egy olyan útra, mely fogalmakkal le nem írható, aki a felszínben, a közvéleményben, a mindennapok fellengzős szavaiban és eszményeiben hisz, azt nem gyarapítják eseményei. Azt az események tartják hatalmukban, nem ő az eseményeket."

Oswald Spengler

A hidegháború lezárását – vagy mai szemmel nézve talán felfüggesztését – követően formálódó gazdasági, társadalmi és geopolitikai környezetben a biztonság és védelem témakörei hátrébb sorolódtak egy időre a prioritások listáján. A Szovjetunió összeomlását követő „fellélegzés" után azonban történelmi léptékben gyorsan következett az az időszak, amikor a biztonsági környezet dinamikus és sok tekintetben negatív változásokba kezdett a délszláv válsággal, a nemzetközi terrorizmus megújulásával, a közel-keleti konfliktusokkal, majd a hagyományos hatalmi versengés újraéledésével. Ezek mértéke persze nem hasonlítható a totális háború fenyegetésének rémével kísértő geopolitikai közeghez. A biztonság és védelem fontosságát kevésbé értékelő átmeneti időszak azonban intézményi, politikai és társadalmi mértékben is kellően hosszú volt a maga évtizedes kiterjedésével ahhoz, hogy egy negatív irányú változási trendhez könnyen alkalmazkodóvá tegyen minket.

A biztonság helyén kezelését, annak a társadalmi működés, az államszervezés és a szabályozás terén való megfelelő megjelenítését nehezítette a változások jellege is. Az 1990-es évek végétől ugyanis nem egy nagy és átfogó fenyegetéssel kellett szembenézni, hanem fokozatosan épült fel egy olyan kihívás- és fenyegetésmátrix, ami sok és egymástól eltérő, változó és jószerével kiszámíthatatlan intenzitású problémakörből adódott össze. Ezek összértékének potenciális fenyegetési mértékét a társadalmi biztonságra, illetve az állami-társadalmi reagálóképességre nézve sokáig messze eltérően értékelték a védelmi-biztonsági szakemberek és a többi szféra képviselői. Ez önmagában nehézséget jelentett abban, hogy a változó fenyegetések kezelésére a lehető leghatékonyabb felkészülés kezdődjön. Az erőforrások elosztásától az intézmények létrehozásán és átalakításán át a jogi keretek kialakításáig érezhető volt a biztonságpercepcióban rejlő különbség a többségi társadalmi gondolkodás és

a védelmi szektor között. Be kell persze vallanunk, ez valahol érthető, is és kockázatok terén a legtöbb diszciplínára nézve feltehető, hogy hasonlóan igaz, már csak a szakértelemmel járó többlettudás miatt is. Ez esetben azonban a történelem több ponton igazolta, hogy a biztonság fenntartása olyan prioritás, ami korszakos változások előtt áll, fenntartva a régi idők – akár háborúvá is fajuló – nehézségeit, de teljesen új horizontokat is megnyitva.

A 90-es évekkel kezdődő időszak ugyanis többes átalakulást is magával hozott. A kapitalista világrendszer új szintre lépése és vele a fogyasztói társadalom jelentős felerősödése a transzatlanti térségben egyértelműen átalakította az egyéni és társadalmi világlátást. Az ezzel párhuzamosan zajló infokommunikációs fejlődés és különösen a digitalizáció dinamikája és széles körű – már-már az életviszonyok nagy részét érintő vagy átható – terjedése pedig további jelentős hatásokat gyakorolt az életvitelre és vele a társadalmi szintű működésre. Ennek tovagyűrűzése ma már átjárja a termelést, a szolgáltatásokat, az oktatást, a tudományt, a politikai kultúrát és intézményrendszert és szükségképpen a biztonságot is, hiszen az új – digitális – szféra vagy dimenzió egyértelműen újfajta biztonsági kockázatokat is generált.

Akkor tehát, amikor a jelen kötet alapját adó kutatásokra felkértük az egyes szerzőket, feltett szándékunk volt, hogy az elmúlt évtizedek jelentős és többrétű változásai kapcsán olyan tágabb társadalmi, állami, jogi és politikai képet rajzoljunk fel, amely segít a kibertérben és a mesterséges intelligenciában rejlő kihívásokat egy a kor komplexitásához közelítő keretben elhelyezni. Alapvetésünk volt, hogy a kibertér vonatkozásában – annak differenciáltságából és szakadatlan fejlődéséből adódóan – sem adhatók leegyszerűsítő, egyes adott konkrétumokra irányuló válaszok. A kötet célja ezért támogatni a digitális fejlődéssel kapcsolatos biztonsági vonatkozások transzatlanti államisághoz illeszkedő fejlesztését a tudomány különféle területekre irányuló vizsgálataival.

Bízunk abban, hogy szerzőink munkája segíteni tudja majd a további kutatásokat, illetve lehetőség szerint támogatást tud nyújtani a témakörökkel kapcsolatos jövőbeni képzések, szakmai, szakpolitikai és szabályozási problémák azonosítása és esetleges megoldása terén is. Ahogy ugyanis korábbi kutatásaim során is vallottam, a múlt megoldásai közül megtartandók a ma is jól fungáló elemek, de a pillanatnyi kihívásra reagáló módosítások nehezen tudják egy hosszabb időszak eredményességét szolgálni, úgy a kibertér és a mesterséges intelligencia biztonsági vonatkozásai kapcsán is úgy hiszem, a konkrét kérdések megválaszolásához előbb hátrébb kell egyet lépnünk. Rendszerszinten kell megvizsgálnunk, hogy maguk a nagybani keretek mennyire alkalmasak az új környezet kezelésére, és hogy magukat a kereteket mennyiben formálják az új közeg erőhatásai.

Jelen kötetben sokféle téma kapcsán jelennek meg ilyen irányultságú, áttekintő írásművek. Ezek mindegyikéről azt gondolom, hogy még a konkrétabb témák és információk is magukban rejtik a szélesebb horizontra való absztrahálhatóság lehetőségét, és ezzel segíteni tudják a jövőbeni biztonság fokozását. Ennek pedig

előfeltétele a mottóul választott Spengler-gondolat magja, jelesül, hogy a kort következtésük meg, és benne a különféle szférák, szakterületek bonyolult egymásmellettiségét és egymáshoz kapcsolódását is. E nélkül ugyanis valóban az események foglyai leszünk, esetről esetre reagálunk majd, mígnem eljön egy – aktuálisan épp a Covid19 világjárványhoz, esetleg az orosz–ukrán háborúhoz hasonló vagy épp azt messze meghaladó – olyan krízis, amelyre már csak történelmileg is drasztikus léptékű változásokkal és ebből következő számos új bizonytalansággal, feszültséggel és áldozatvállalással lehet reagálni. Persze minden veszélyre nem lehet tökéletesen felkészülni, és nem lehet folyamatos félelemérzetre sem stabilan építkezni, de úgy hiszem, egy biztonságtudatosabb, valamint a 90-es és a 2000-es évek elejének szellemiségével ellentétben a különféle szakterületek közti kölcsönös megértésre törekvésen alapuló együttműködéssel egy alkalmazkodóképesebb, divatosan: reziliensebb és ebből adódóan hatékonyabb, termelékenyebb, innovatívabb és mégis stabilabb jövőt építhetünk.

A szerkesztők

KELEMEN ROLAND

Cyberfare State modelljei

A digitális állam lehetséges irányai

Annak a gondolata, hogy a kibertér és a hozzá kapcsolódó rendszerek felhasználhatóak az állam működése során, az egyes alrendszerek pedig eredményesebbé válhatnak ezáltal, nem új keletű gondolat. *Gregory M. Kaladijan 1996-os* Journal of Children and Poverty*ben megjelent Welfare vs. Cyberfare című cikkében arra vállalkozott, hogy a welfare state (jóléti állam) reformjának szükségét felvázolja. A tanulmányban az elektronikus rendszerek szociális igazgatásban történő felhasználása mellett érvelt,* melyek a már működő szociális struktúrát véleménye szerint átláthatóbbá és igazságosabbá, a rendszer működését pedig ezáltal eredményesebbé tették volna.[1]
Kaladijan a kibertér fejlődésének egy korai időszakában ismerte fel annak államigazgatást, állami alrendszereket, az állami funkciókat hatékonyabbá tevő képességét, igaz, ő csak egy területre, a szociális igazgatásra és annak hosszú ideje visszásan működő rendszerének megújítására látott benne fantáziát. Szavai azonban akkor – valószínűsíthetően a fókuszált terület társadalmi érzékenysége és a kibertér fejlődésének korai szakasza okán – lényegi változást nem eredményeztek. Mára viszont az államigazgatás teljes rendszere, így vagy úgy, de megjelent a kibertérben, a gazdasági szereplők tevékenysége elképzelhetetlen a virtuális tér nyújtotta lehetőségek nélkül, az emberek pedig a hétköznapjaik nagy hányadát töltik e közegben. Ez azonban nem egyszerűen a welfare state reformját eredményezte, azon lényegesen túlmutat hatásában, hiszen egy teljesen átalakult struktúrájú társadalmi-gazdasági közeget hozott létre ez a folyamat, amely az állami funkciók összességét is érintette. E folyamat alapjaiból kiforgatta a társadalmi totalitás egészét,[2] így annak minden egyes részkomplexumát: a gazdaságot, a jogot, a közigazgatást és a fegyveres védelem ágazatait[3] is.

Az „evolúció" sajátja, hogy nemcsak a welfare state jegyeit vette át, módosította és szelektálta a szereplők hatalmi igényei szerint, hanem a geopolitikai környezet átalakulásának és a technológiafejlődés jelentette biztonsági problémáknak köszönhetően

[1] Tanulmányát lásd Gregory M. Kaladijan: Welfare vs Cyberfare. *Journal of Children and Proverty*, 1996/1. szám, 93–104. o.

[2] Peschka Vilmos: *A jog sajátossága.* Budapest, Akadémiai Kiadó, 1988, 33. o.

[3] Farkas Ádám: *A fegyveres védelem mint állami alrendszer és annak szabályozási sajátosságai.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2018; Farkas Ádám: *Az állam fegyveres védelmének alapvonalai.* Budapest, Katonai Nemzetbiztonsági Szolgálat, 2019.

egyes államok visszanyúltak a warfare state (hatalmi állam) jegyeihez is. Warfare state esetében ki kell emelni, hogy ez nem a jó állammal – welfare state-tel – szemben álló rossz állam, hanem olyan államfejlődési stáció(k), amely(ek) megjelent(ek) a transzatlanti térség államaiban is. Jelentősége abban fogható meg, hogy az államot ért impulzusokra, kiemelten a biztonságot érintő társadalmi vagy külső hatásokra való válaszreakcióként megjelenő állami (működési, szervezeti, funkcionális) racionalizációt, a védelmi, biztonsági aktorok centralizációját jelentette.[4] Bruce D. Porter tanulmányában az Egyesült Államok államfejlődésével kapcsolatban ki is fejtette, hogy ez az államfelfogás kellett az erős szövetségi állam létrejöttéhez, mivel a külső – vagy a polgárháborús – fenyegetettség minden esetben szükségessé tette az állam működésének átgondolását, adott esetben racionalizálását.[5] Emellett azonban nem elhallgatható, hogy ezen államfelfogás az 1945 előtti nemzetközi jogi környezetben kedvezett a nemzetközi konfliktusok eszkalálódásának, ha a jogállami kereteket nem tudták megerősíteni, illetve garantálni a békés működést.

A 21. század első évtizedeiben világossá vált, hogy a digitalizáció jelentős hatást gyakorol a társadalmakra, az államra, annak minden funkciójára. A pozitív hatások erősítik a jóléti funkciókat, emellett számos területen fejtenek ki jótékony hatást (lásd kommunikáció, okos városok stb.), mindazonáltal a negatív oldala is egy újfajta fellépést kíván az állam intézményeitől, védelmi-biztonsági funkcióitól, de társadalmi-politikai konstruktumaitól is.

Jelen tanulmány célja, hogy bemutassa a kibertér államra és állami alrendszerekre gyakorolt hatását, mind pozitív, mind pedig negatív oldalról; mivel kizárólag ez eredményezheti egy olyan átfogó kép megalkotását, mely révén megfelelő jogi, biztonsági válaszokat tudunk adni a kialakult vagy kialakulóban lévő folyamatokra.

1. A KIBERTÉR ÁLLAMRA GYAKOROLT HATÁSA

1.1. A welfare sate digitalizációja, a technológia pozitív hatása a 21. század államára

A jóléti állam a szervezett kormányzati hatalom tudatos alkalmazását jelenti annak céljából, hogy a piaci erőhatásokat valamiféle társadalmi igazságossági és elosztási eszmény mentén módosítsák. Ezt kifejezetten három területen kívánták érvényre juttatni: (1) egyéneknek és családoknak minimális jövedelmet garantálva (munká-

[4] Lásd: James T. Sparrow: *Warfare State – World War II Americans and the Age of Big Government.* Oxford, Oxford University Press, 2011.

[5] Bruce D. Porter: The Warfare State. *American Heritage*, 1994/4. szám (https://www.americanheritage.com/warfare-state#1); Bruce D. Porter: *War and the Rise of the State – The Military Foundations of Modern Politics.* New York, The Free Press, 1994, 7. fejezet War and the American Goverment.

tól, munkabértől függetlenül); (2) szűkíteni a gazdaság bizonytalanságait, és ezzel elérve bizonyos társadalmi kockázatok kezelését; (3) meghatározott szolgáltatások esetében a lehető legmagasabb szintű ellátás biztosítása. Az első kettőt már korlátozottan, de a szociális állam is képes volt megvalósítani.[6] Azonban a harmadik cél ezen állammodellen már túlmutatott, és az egyenlő bánásmód irányába kívánta módosítani a rendszert. Ez pedig a piacgazdaság negatív hatásainak a figyelem középpontjába kerülése miatt történhetett meg, hiszen szükségessé vált azok enyhítése, rendezése. Azonban, eltérően a szociális államtól, már nem a minimum garantálására törekedett, hanem az optimum irányába mozdult el a rendszer.[7]

Magának a jóléti államnak létrejöttét a fenti felismeréseken túl több tényező együttállása tette lehetővé, így kifejezetten: az általános választójog kialakulása; a politikai demokrácia kompetitív logikája; a korábbinál tagoltabb és komplexebb társadalmi rétegződés; az érdekcsoportok növekvő befolyása; valamint a szocialista államodellek jóléti ígéreteivel szembeni hatékony alternatíva állítása.[8] Ezen államodell „a demokratikus jogok kiterjesztése és kiszélesítése részeként komplex jóléti rendszereket alakított ki…".[9] Ezzel pedig több funkciót kívánt érvényre juttatni, így többek között a társadalom által okozott, azonosítható hátrányok enyhítését (munkanélküliség, üzemi balesetek, háborús nyugellátás stb.), a társadalom által nehezen azonosítható, vis maior jellegű hátrányok tompítását (légszennyezés, városok pusztulása), indokolatlan társadalmi hátrányok kompenzációját (pl. szolgáltatás a hátrányos helyzetű gyermekek részére), valamint befektetést a jövő generációiba (pl. oktatás), továbbá a személyes jólét alapfeltételeinek megteremtését (saját ingatlan, közművek stb.).[10] Megvalósítás eszközeként fogható fel a társadalombiztosítás, a pénzbeli juttatások, a természetbeni juttatások, a partnerségi együttműködés kialakítása egyes szervekkel és a helyi önkormányzatok szociális tevékenységének erő-

[6] Lásd többek között Szépvölgyi Enikő: A dualizmuskori állami gyermekvédelem és a szegénység összefüggései. *Jog Állam Politika*, 2020/3. szám, 101–116. o.; Szépvölgyi Enikő: Gondolatok az állami gyermekvédelemről szóló törvénycikkek 120. évfordulójára. In Mezey Barna (szerk.): *Kölcsönhatások. Európa és Magyarország a jogtörténelem sodrásában.* Budapest, Gondolat Kiadó, 2021, 316–323. o.; Kelemen Roland: A polgári kor társadalombiztosítása – Társadalombiztosítási bíráskodás a polgári korban. In Molnár Andrea – Széplaki László (szerk.): *Tanulmányok a győri felsőbíráskodás történetéből a XIX–XX. század fordulóján.* Győr, Győri Ítélőtábla, 2019, 149–174. o.

[7] Asa Briggs: The Welfare State in Historical Perspective. In Christopher Piersen – Francis G. Castel (szerk.): *The Welfare State Reader (Second Edition).* Cambridge, Polity Press, 2006, 16–17, 27. o.

[8] Pongrácz Alex: *Nemzetállamok és új szabályozó hatalmak a globális erőtérben – avagy megszelídíthető-e a globalizáció?* Budapest, Dialóg Campus, 2019, 55. o.

[9] Pongrácz Alex – Téglási András: Szociális állam, jóléti állam – Elméleti és történeti alapvetés. In Bódi Stefánia – Schweitzer Gábor (szerk.): *Az emberi jogok alkotmányos védelme Magyarországon.* Budapest, Ludovika Egyetemi Kiadó, 2021, 299. o.

[10] Richard Titmuss: Universal versus Selection. In Christopher Piersen – Francis G. Castel (szerk.): *The Welfare State Reader (Second Edition)*, Cambridge, Polity Press, 2006, 42–43. o.

sítése.[11] Az eszközök szerkezetére, tartalmára eltérő megoldások születtek az államról való gondolkodás, a társadalmi tradíciók és a történelmi hagyományok nemzeti sajátosságai mentén.[12] Az érintett területek, szakpolitikák köre soha nem rögzült taxatív módon, azok folyamatos változásokat mutatnak, igazodva az adott kor aktuális kihívásaihoz is.

A 21. század társadalmi folyamatai ismét próbára teszik a jóléti rendszerek és az állam alkalmazkodóképességét. Így például a munka világában megjelenő, szolgáltatásalapú gazdaság jelentős változásokat eredményez. A World Economic Forum szerint 2015–2020 között közel 7,1 millió állás szűnt meg 15 gazdasági ágazatban.[13] Ez pedig csak az első lépés volt, ugyanis szintén WEF által kiadott dokumentum, a *Future of Jobs 2020* című jelentésében található becslés szerint 2025-re 85 millió munkahely szűnik meg, mert a gépekkel olcsóbb és hatékonyabb lesz az egyes feladatok ellátása, ezzel párhuzamosan pedig kialakul 97 millió új típusú feladat, szerepkör,[14] amelyek alapja a hatékonyabb alkalmazkodás az emberek és gépek közötti interakciókban.[15] Horváth Zoltán a Széchenyi István Egyetem Gépészmérnöki, Informatikai és Villamosmérnöki Kar dékánjának a szavai mutatják, hogy ez a folyamat a következő években nemhogy nem enyhül, hanem rohamtempóra fog kapcsolni. Beszéde szerint ugyanis – amit SZE GIVK diplomaátadóján mondott – „a társadalom- és jövőkutatók szerint harminc év múlva a szakmák nyolcvan százaléka olyan lesz, ami most még nem is létezik. Nagy eséllyel Önök olyan szakmában dolgoznak majd, ami jelenleg még nincs is, csak elképzelésünk van róla."[16] Ennek természetszerűleg részét képezi a munkahelyi környezet átalakulása, hiszen a vállalkozások szükségszerűen költséghatékonyságra törekednek, amelynek egyre inkább részét képezi a demonetizáció mint digitális következmény: vagyis a növekvő digitalizációs szint kevesebb fizikai költséghez vezet,[17] ami versenyelőnyt eredményez egyik oldalról,

[11] Briggs: i. m. (2006) 18. o.

[12] Gøsta Esping-Andersen: Towards the Good Society, Once Again? In Gøsta Esping-Andersen (szerk.): *Why We Need a New Welfare State.* Oxford – New York, Oxford University Press, 2002, 1. o.

[13] Ferencz Jácint: Az információ és a technológia kettős arca a munkajogban. In Baranyiné Kóczy Judit – Fehér Ágota (szerk.): *Pedagógusképzés, oktatás a Kárpát-medencében, társadalmi kontextusok. XXII. Apáczai-napok Tudományos Konferencia tanulmánykötet.* Győr, Széchenyi István Egyetem Apáczai Csere János Kar, 2019, 322. o.

[14] Ezt igazolja vissza a robotika területe is. Lásd Hajdú József: A mesterséges intelligencia hatása a munkaerőpiacra, avagy elveszik-e a robotok az ember munkáját. *Infokommunikáció és Jog,* 2020/2. szám, 3–9. o.

[15] *The Future of Jobs Report 2020 – October 2020.* World Ecnomic Forum (https://www3.weforum.org/docs/WEF_Future_of_Jobs_2020.pdf), 5. o.

[16] Nimsz Zsuzsanna: Szombaton is sokan vették át a diplomájukat a SZE-n. *Győr+,* 2022. 07. 17. (https://www.gyorplusz.hu/gyor/szombaton-is-sokan-vettek-at-diplomajukat-a-sze-n/)

[17] Gyekiczky Tamás: *Olvasmányok a Digitális társadalomról – jogászoknak* (kézirat). Budapest, 2021, 112. o. (https://www.academia.edu/49694295/Olvasm%C3%A1nyok_a_Digit%C3%A1lis_T%C3%A1rsadalomr%C3%B3l_Jog%C3%A1szoknak).

másik oldalról az okos munkahelyek megteremtése egyes hagyományos szakmák megszűnését eredményezheti, de legalábbis átképzést, fejlesztést követel meg. Így a tudás- és készségintenzív gazdaság hátrányos társadalmi következményeinek elkerülése érdekében az államnak jelentős beruházásokat kell eszközölnie ezen csoportok oktatására, átképzésére.

A változó és fejlődő technológiák, a fokozódó globális integráció és az ezekhez való alkalmazkodás képessége, a szolgáltatószektor túlságos dominanciája és az általa szült tudásintenzív gazdaság együttesen szakadékot teremtenek társadalmakon belül, illetve ezek a tendenciák az államok között is fokozzák a polarizáltságot. Szükségszerűvé vált az államról alkotott felfogásunk újragondolása is.[18] „A szabadversenyes korszak be nem avatkozó, éjjeliőr államával szemben – amely az állami szerepvállalást a közrend és a közbiztonság fenntartására és a gazdaság működési feltételeinek biztosítására korlátozta – a jóléti állam tevékeny állam volt."[19] E megváltozott, az államot aktív cselekvésre ösztönző környezetben kézenfekvő, hogy eme jóléti állam egyes attribútumait erősítő államfelfogás tud csak eredményesen fellépni a korszak kihívásaival szemben.

Ennek egyik úttörője volt a bevezetésben már citált Kaladijan is, aki a jóléti állam reformjának lehetőségét a digitalizációban látta. A technológia hihetetlen fejlődése a 21. század első évtizedeiben arra a szintre jutott, hogy az élet szinte minden területén megkerülhetetlen tényezővé vált. Ebből a fejlődésből is kiemelkedik a kibertér által generált lehetőségek és változások tárháza, amelynek köszönhetően Kaladijan eszménye a digitálisan hatékonyabbá, igazságosabbá tett jóléti rendszerről részint megvalósulni látszik. Ez szintén a jóléti államok sajátos államfelfogásán is alapszik, hiszen annak megteremtése a társadalom oldaláról igényt támasztott a minőségi közigazgatás kialakítására, fejlesztésére; „a közigazgatás ennek következtében megszűnt a jogszabályok puszta végrehajtója és a hatósági jogalkalmazó közigazgatás kizárólagos terepe lenni",[20] létrehozva ezzel a szolgáltató közigazgatást. Így a technológia forradalma a jóléti állam szükségszerű átalakulását is eredményezi, tehát szintén szükségszerűen magával hozta a közigazgatás, végső soron a teljes államműködés reformját is.

Az állami intézményrendszernek fel kellett vennie a versenyt az átalakult szolgáltatóiparral, amely lehetővé tette, hogy a saját otthonainkból szinte minden elérhetővé váljon az okoseszközök használatának köszönhetően. Az e-közigazgatás fokozatos kialakításával és fejlesztésével lépett e verseny pástjára az állam, amelynek köszönhe-

[18] Gøsta Esping-Andersen: A Welfare State for the Twenty-first Century. In Christopher Piersen – Francis G. Castel (szerk.): *The Welfare State Reader (Second Edition)*, Cambridge, Polity Press, 2006, 434, 447–448. o.

[19] Szigeti Péter: *Társadalomkutatás – Mi végre? Politikatudomány, alkotmányjog, világrendszerelmélet*, Győr, Universitas, 2011, 262. o.

[20] Pongrácz i. m. (2019) 163. o.

tően hatékonyabbá, naprakészebbé és nem utolsósorban polgárbaráttá (felhasználóbaráttá) vált a rendszer.[21] Az egyes szolgáltatások könnyebben elérhetővé váltak,[22] és a legtöbb esetben az eljárások is jelentősen felgyorsultak.

Az átalakulás azonban itt nem állt meg. A kibertér megjelenése a Titmuss fentebb ismertetett állami (jóléti) funkcióinak valamennyi szegmensére hat, hatott. A kibertéren alapuló technológiai újítások robbanásszerű változásokat idéztek elő, illetve előrevetítenek olyan generális átalakulásokat a tudományos vagy társadalmi alrendszerekben, amelyek révén az emberiség óriási lépéseket tehet az eddig megoldhatatlan problémák kezelése tekintetében.[23] Jól illusztrálja ezt a kvantumszámítógépek megjelenése és folyamatos, gyors fejlődése és hasznosíthatósága is. Az első, 2019-ben a Google által fejlesztett gép 54 qubites processzorra épült, amely 200 másodperc alatt végzett el olyan műveletet, amely a korábbi technológiai csúcsot jelentő szuperszámítógépeknek tízezer évbe telt volna.[24] Alig telt el három év, és 2022 őszén az IBM bejelentette Osprey nevű kvantumszámítógépét, amely 433 qubittel rendelkezik. Ezen gépek sajátja, hogy „a kvantumbitek a hagyományos bitekkel ellentétben egyszerre vehetik fel a 0, az 1 vagy akár egyszerre mindkettő értékét, ami lehetővé teszi olyan számítások elvégzését, amelyek még a legmodernebb szuperszámítógépeknek is túl bonyolultak – ilyen például a kémiai reakciók szubatomi részletességgel történő szimulálása"[25]. Amúgy az Egyesült Államok és Kína között e területre is kiterjed a verseny; Kína 2021-ben jelentette be a világ akkori legnagyobb teljesítményű kvantumszámítógépét, így feltételezhetjük, hogy a távol-keleti állam esetében sem ez volt a fejlesztés csúcsa.[26] Hasonló volumenű fejlesztés a kaliforniai Stanford Egyetemen működő Stanford Linear Accelartor Center laboratóriumában kifejlesztett óriás digitális kamera, amely 189 érzékelőt tartalmaz, és 3,2 gigapixelre képes. Az eszköz a távoli galaxisok feltérképezését fogja segíteni, és várhatóan 20 milliárd galaxist fog katalogizálni, eközben éjszakánként 15 terabájtnyi adatot gyűjt. Az eszköznek köszönhetően a kutatók közelebb kerülhetnek az univerzum kialaku-

[21] Lásd Budai Balázs: *Az e-közigazgatás fogalma, jogi és stratégiai keretei.* Budapest, Dialóg Campus, 2017.

[22] Gondoljuk itt például Magyarország tekintetében az internetes ügyfélkapurendszerre, amelynek köszönhetően számos szolgáltatást az otthonunkból ki sem mozdulva tudunk elérni.

[23] Yuval Noah Harari: *Homo Deus. – A holnap rövid története.* Budapest, Animus Kiadó, 2016.

[24] Bognár Zsolt: Egy új korszak kezdete: A Google elérte a kvantumfölényt. *Qubit,* 2019. 09. 24. (https://qubit.hu/2019/09/24/egy-uj-korszak-kezdete-a-google-elerte-a-kvantumfolenyt).

[25] Bognár Zsolt: Az IBM megépítette a világ legnagyobb, 433 qubites kvantumszámítógépét. *Qubit,* 2022. 11. 09. (https://qubit.hu/2022/11/09/az-ibm-megepitette-a-vilag-legnagyobb-433-qubites-kvantumszamitogepet).

[26] Bognár Zsolt: Kína bemutatta a világ legnagyobb teljesítményű kvantumszámítógépét. *Qubit,* 2021. 07. 14. (https://qubit.hu/2021/07/14/kina-bemutatta-a-vilag-legnagyobb-teljesitmenyu-kvantumszamitogepet).

lásának megértéséhez, illetve az univerzum és a sötét anyag működése hátterének feltérképzéséhez.[27]

Kézzelfogható eredményeket lehet felmutatni az oktatásban, kutatásokban, az egészségügyben, a szociális szférában, ahol megjelent az IoT[28], az IoD[29] és az okoseszközök,[30] a mesterséges intelligencia pedig egyre jelentősebb teret foglal el. A kibertérhez csatlakozó eszközök (az állam, a gazdaság és az egyén oldaláról), valamint a korábbi évszázadok tudásának és a folyamatoknak, tevékenységeknek a digitalizálása, óriási adatmennyiséget (big data) generálva, forradalmi átalakulást hoztak a fenti területeken is.

Ez az egészségügyben többek között csökkentette a diagnosztikából eredő hibákat, lehetővé tette a korábban fel nem fedezett összefüggések felismerését, új módszerek kidolgozását, alkalmazását.[31] Ezek közül érdemes kiemelni pár példát. A Semmelweis Egyetem részvételével valósult meg az a kutatás-fejlesztési tevékenység, amelynek köszönhetően a mellkasi CT-felvételeket kiértékelő mesterséges intelligencia felhasználásával javul a korai daganatos megbetegedések felismerésének a lehetősége.[32] A digitalizáció e területen is átalakítja a hagyományos interakciókat, így az orvos-beteg kapcsolatot is. Ennek egy területe az E-Health rendszer, ami arra hivatott, hogy könnyebbé tegye az egészségügyi szolgáltatásokhoz való hozzáférést például az alacsonyabb jövedelműek részére, vagy akik a központoktól távolabb élnek, ezzel pedig a rendszer infrastrukturális hiányosságait próbálja orvosolni.[33] Forradalminak hat az okostelefonok bevonása a mentális betegségek nyomon követése, felmérése és felismerése területén is, mivel az eszközökre telepített alkalmazások ré-

[27] Kun Zsuzsi: A világ legnagyobb 3,2 gigapixeles digitális kamerája magasabb egy autónál, és galaxisok milliárdjait örökítheti meg. *Qubit,* 2022. 10. 28. (https://qubit.hu/2022/10/28/a-vilag-legnagyobb-32-gigapixeles-digitalis-kameraja-magasabb-egy-autonal-es-galaxisok-milliardjait-orokitheti-meg).

[28] Korunk egyik nóvuma, konvergáló technológiája a tárgyak internete (IoT – Internet of Things), amely az információtudomány fejlődésével, a szenzorok használatának fokozódó térnyerésével (ami magával hozza az árak rapid csökkenését) egyre inkább a mindennapi életünk részévé válik mind az otthonokban, mind pedig a közszférában. Lásd Németh Richárd: Kibertámadások gazdasági vonatkozásai a vállalati szférában. In Dernóczy-Polyák Adrienn (szerk.): *Kutatási jelentés 1. Győr.* Universitas-Győr Nonprofit Kft., 2019, 307–325. o.

[29] Baranyi Péter – Csapó Ádám – Budai Tamás – Wersényi György: Introducing the Concept of Internet of Digital Reality – Part I. *Acta Politechnica Hungarica,* 2021/7. szám, 225–240. o.; Baranyi Péter – Csapó Ádám – Budai Tamás – Wersényi György: Internet of Digital Reality: Infrastructural Background – Part II. *Acta Politechnica Hungarica,* 2021/8. szám, 91–104. o.

[30] G. Karácsony Gergely: *Okoseszközök – okos jog?* Budapest, Ludovika Egyetemi Kiadó, 2020.

[31] Bőgel György: *A big data ökoszisztémája.* Budapest, Typotex, 2015, 22–24. o.

[32] Mesterséges intelligencia segíti a tüdőrák hatékonyabb felismerését. *Semmelweis Egyetem – A Semmelweis Egyetem polgárainak lapja,* 2022. október, 18. o.

[33] Incze Norbert – Pesuth Tamás: E-Health – Digitalizálódik az egészségügy? *Köz-Gazdaság,* 2020/4. szám, 247–250. o.

vén lehetőség van valós idejű értékelésre.[34] Hasonlóan eredményesnek mutatkozik a mesterséges intelligencia a járás elemzésében is, ahol meglehetősen hatékonyan szűri ki a kóros járást, így segítve egyes betegségek felismerését.[35]

Az oktatásban és kutatásban is lehetővé vált, válik a modern, kibertérhez kapcsolódó technológia alkalmazása. Az okoseszközök használata és algoritmusok révén a személyre szabott tanulás, tudásanyag átadása komoly potenciált jelent.[36] Ennek az egyik legvitatottabb megjelenési formája Kínához köthető, ahol kísérleti jelleggel megkezdték olyan EEG (elektromos aktivitást mérő elektroenkefalográf) használatát, amely iskolai órák közben vizsgálja a tanulók agyi funkcióit. Az eszköz segítségével a tanár valós időben látja, hogy a gyermek megfelelően koncentrál (fehéren világít a led), vagy unatkozik, mással foglalkozik (pirosan világít a led). A rendszerhez tartozik egy kamerarendszer is, ami a pontosabb képalkotáshoz szükséges. Az adatokból mind az oktatók, mind pedig a szülők valósidejű képet kapnak a gyermekek figyelmi szintjéről. De Kína emellett fejleszti és teszteli az óvodai óvórobotokat, valamint a mesterségesintelligencia-alapú intelligens tutorokat is. Az Egyesült Államokhoz köthető a TAL, amely cég azon dolgozik, hogy az egyéni fejlesztésekre kerüljön a hangsúly, a valós időben adatokat szolgáltató rendszernek köszönhetően, amelyben az MI inkább digitális asszisztens szerepét tölti be.[37] India Kínához hasonlóan hatalmas lehetőséget lát az oktatás digitalizációjában, és óriási forrásokat költ arra, hogy az oktatás minél nagyobb területén jelenjenek meg az okoseszközök.[38] A big datának köszönhetően a kutatások soha nem látott, országhatárokat átlépő, kontinenseket összekötő hálózatokat generálnak, felgyorsítva az innovációt. Ezen innovációnak a gyorsaságát mutatja, hogy Moore-törvénye,[39] amely szerint az in-

[34] Tanyi Lakhtakia – Ameya Bondre – John Torous et al.: Smartphone digital phenotyping, surveys, and cognitive assessments for global mental health: Initial data and clinical correlations from an international first episode psychosis study. *Digital Health*, 2022/november (https://journals.sagepub.com/doi/10.1177/20552076221133758).

[35] Ashley Cha Yin Lim – Pragadesh Natarajan – R. Dineth Fonseka – Monish Maharaj – Ralph J. Mobbs: The application of artificial intelligence and custom algorithms with inertial wearable devices for gait analysis and detection of gait-altering pathologies in adults: A scoping review of literature. *Digital Health,* 2022/január (https://journals.sagepub.com/doi/full/10.1177/20552076221074128).

[36] Tilesch György – Omar Hatamleh: *Mesterséges intelligencia – Vegyük kezünkbe a sorsunkat az MI korában.* Budapest, Librid, 2021, 65–68. o.

[37] Kolozsi Ádám: Beelektródázták a gyerekeket az iskolapadban. *Index,* 2019. 11. 14. (https://index.hu/techtud/2019/11/14/mesterseges_intelligencia_kina_oktatas/).

[38] K. Seethal – B. Menaka: Digitalisation Of Education In 21ST Century: A Boon Or Bane. *International Journal for Research in Engineering Application & Management,* 2019. (http://www.ijream.org/SpecialIssueConference/ICDOMP2019036.pdf).

[39] Gordon E. Moore: Cramming more components onto integrated circuits. *Electronics,* 1965/8. szám.

tegrált áramkörök összetettsége körülbelül 18 havonta megduplázódik, napjainkban egyre inkább megdőlni látszik, hiszen ez a tendencia gyorsulóban van.[40]

Úgyszintén domináns a diszruptív technológiák térnyerése, amely még összetettebbé, sérülékenyebbé, de látszólag mindenképpen könnyebbé teszi az emberek hétköznapjait,[41] így a dolgok internetéhez 2020-ban már több mint 26 milliárd eszköz csatlakozott. A mesterséges intelligencia pozitív hatásai a technológiai fejlődéssel 2030-ra megsokszorozódnak. A Stanford Egyetem által közzétett előrejelzés szerint a mesterséges intelligencián alapuló innováció majd elérhetővé teszi, hogy még összetettebben működő okosvárosok jöjjenek létre, ahol autonóm járművek könnyítik az utazást, az áruszállítást,[42] és az orvosi diagnosztika területén a vérnyomást, vércukorszintet és egyéb jellemzőket monitorozó, adatokat gyűjtő szenzorok a páciensek életét menthetik meg.[43] A gyorsuló megtérülés törvénye[44] pedig csak erősíti ezt a folyamatot, hiszen elvárja, hogy új technológia jöjjön létre, ami gyorsabb fejlődést eredményez, és az természetszerűleg még újabb technológiákat szül. Ez pedig öngerjesztő folyamat, pozitív visszacsatolást generál, amely következtében az egyik részterület gyorsítja a másik terület fejlődését, például a robotika, MI, kvantum- és nanotechnológiák, bioinformatika, blokkláncok, VR területén és így tovább.

Azonban az állam működésének átalakulása nem állt meg a jóléti rendszerek modernizálásánál, a modern technológia alapjaiban alakította át a teljes állami működési mechanizmusokat, valamint az állam és a gazdasági szereplők, továbbá az állam és a polgárok közötti interakciókat. A modern technológia ennek köszönhetően behatolt az élet minden szintjére és azokra jelentős hatást gyakorolt, így egyebek

[40] Justin Viktor: Vajon valóban elbukik a Moore-törvény, vagy van még tovább? *Rakéta,* 2021. 04. 30. (https://raketa.hu/vajon-valoban-elbukik-a-moore-torveny-vagy-van-meg-tovabb).

[41] Debashis Majumdar – Pradipta Kumar Banerji – Satyajit Chakrabarti: Disruptive technology and disruptive innovation: ignore at your peril!: *Technology Analysis & Strategic Managment,* 2018/11. szám, 1247–1255. o.

[42] Boris Bucko – Martin Michálek – Katarina Papierniková – Katarína Zábovká: Smart Mobility and Aspects of Vehicle-to-Infrastructure. *Applied Sciences,* 2021/11. szám (https://www.mdpi.com/2076-3417/11/22/10514/htm); Mariam Fandáková – K. Zabovska – Boris Bucko – Michal Zábovsky: Improvements of Computer Assisted Virtual Environment (CAVE). *2020 43rd International Convention on Information, Communication and Electronic Technology (MIPRO)*, 2020, 1680–1684. o.

[43] Tom Abate: Smarter Hospitals: How AI-Enabled Sensors Could Save Live. *HAI Stanford University Human-Center Artificial Inteligence,* 2020. 09. 09. (https://hai.stanford.edu/news/smarter-hospitals-how-ai-enabled-sensors-could-save-lives). Jessilyn Dunn – Lukasz Kidzinski – Ryan Runge at. al.: Wearable sensors enable personalized predictions of clinical laboratory measurements. *Nature medicine,* 2021, 27. kötet, 1105–1112. o. (https://nmbl.stanford.edu/wp-content/uploads/Dunn-Nature-Med-2021.pdf).

[44] Ray Kurzweil: *A szingularitás küszöbén.* Budapest, Ad Astra, 2014, 58–72. o.

mellett a rendészetre,[45] az igazságszolgáltatásra,[46] a közlekedésre,[47] az energiahasználatra és az önkormányzatiságra[48] és nem utolsósorban a védelem és biztonság világára is.[49]

Ezek a megoldások sok tekintetben sokkal élhetőbbé tették és fogják tenni az emberek hétköznapjait, az állam működését pedig racionalizálják, felhasználóközpontúbbá tették és fogják tenni. Mindemellett azonban a szolgáltatásközpontúság, az adatokhoz, a képességekhez való hozzáférés lehetősége a klasszikus welfare state egyenlőségre törekvő oldalát elmozdította egy elitista működés irányába, ahol ezen erőforrások feletti tényleges rendelkezés lehetősége teremti meg a döntéshozásnak az alapjait.[50] Tökéletes példái ennek a magántulajdonban álló okos városok, ahol az adatok szinte teljességéhez hozzáférnek az olyan nagyvállalatok, mint az Amazon Seattle-ben, vagy Facebookville, Zucktown esetében a Meta, de többek között ilyet tervez létrehozni a Tesla Ausztráliában Yarrabend néven.[51] Szintén az adatok garmadája felett diszponálnak a közösségimédia-vállalatok, azokat tényleges termékként kezelik. *Érdekes módon tehát a nyugati államokban a gazdaság – főként a kibertérben tevékenységet realizáló – transznacionális szereplői tömegesen férnek hozzá az egyénekhez fűződő adatokhoz,*[52] *míg az alkotmányos struktúrájukban kialakított korlátoknak és fékek-*

[45] Lásd Abishur Prakash: *Go. AI – A mesterséges intelligencia geopolitikája.* Budapest, Pallas Athéné Könyvkiadó, 2018, 97–108. o.

[46] Nogel Mónika: Bűnös vagy ártatlan? Igazságügyi genetikus szakértői vélemények relevanciája a védelem számára. *Belügyi Szemle,* 2022/3. szám, 481–503. o.; Vajda János Álmodnak-e az androidok elfogult bírókkal? Kognitív torzítások és önbeteljesítő jóslatok a mesterséges intelligencia peres előrejelzéseiben. *Infokommunikáció és Jog,* 2022/1. szám, 20–22. o.

[47] Atanu Bhuyan: Designing optimal welfare policies for intermediate public transportation systems: A developing country perspective. *Academia Letters. (https://www.academia.edu/44905958/Designing_optimal_welfare_policies_for_intermediate_public_transportation_systems_A_developing_country_perspective).*

[48] Lásd Kovács László: *A kibertér védelme.* Budapest, Dialóg Campus, 2018, 19–118. o

[49] Példaként ebben a körben érdemes megjegyezni, hogy több szerző is kiemelte már a digitális adatokkal történő rendelkezés biztonságra, védelemre gyakorolt hatását, illetve fake news társadalmi kohéziót romboló hatását, továbbá az erre épített dezinformációs tevékenység nemzetbiztonsági vonatkozásait. Lásd Amaël Cattaruzza: *A digitális adatok geopolitikája – A hatalom és konfliktusok a big data korában.* Budapest, Pallas Athéné Könyvkiadó, 2020; Kelemen Roland: Radikalizálás, dezinformálás és tömegpszichózis modern köntösben: a hibrid konfliktus kibertérben. *Jog Állam Politika,* 2021/3. szám, 71–85. o.

[50] Lásd Árva László – Pásztor Szabolcs – Victoria Pyanatova: A multinacionális vállalati stratégiák és a változó világkereskedelem kapcsolatáról. *Gazdaság és Pénzügy,* 2020/1. szám, 57–81. o.

[51] Vincent Mosco: *Okosvárosok a digitális világban.* Budapest, Pallas Athéné Könyvkiadó, 2019, 137–145. o.; Lásd még Dusek Tamás: Az okos városok komplex mutatószámainak egyes tartalmi és módszertani problémái. In Kovács Gábor – Völgyi Katalin (szerk.): *Üzleti vállalkozások, makro- és mikrokörnyezetük gazdálkodási és menedzsment sajátosságai c. kutatás tanulmányai.* Győr, Széchenyi István Egyetem Kautz Gyula Gazdaságtudományi Kar, 2018, 1–3. o.

[52] Ezen vállalatok az adatokhoz való hozzáférést követően nem kizárólag felhasználják ezeket az információkat, hanem kereskedelmi és politikai célokra áruba bocsátják, ezzel is erősítve az adatok

nek köszönhetően az államok számára ezeknek az elérhetősége erősen korlátozva van. Látni fogjuk ezzel szemben, hogy a keleti autoriter államalakulatok maguk is végrehajtották – igaz, sajátos módon – az államaik digitális (jóléti) reformját, addig viszont az adatok lehető legteljesebb köre felett kívánnak rendelkezni.

1.2. A warfare state digitalizációja – A kibertérben realitássá vált totális biztonsági kihívások

A keleti államok, főként Kína és Oroszország jelentős mértékben kiaknázzák a technológiai újításokból fakadó biztonsági képességeket. Ennek eklatáns példája az okos város nyújtotta jóléti lehetőségekbe burkolt totális megfigyelés és adatgyűjtés lehetősége. Ilyen rendszer kiépítését kezdte meg Kína a 2010-es évek elejétől. *Megdöbbentő módon a világban jelenleg futó körülbelül ezer okosváros-projekt közel fele Kínához köthető.* Ennek központi eleme a Citizen Cloud, „ez egy felhőalapú platform, és egyben mobil alkalmazás is, amely egyesíti a kormányzati szolgáltatások legnagyobb részét, és megkönnyíti a városlakók számára az ezekhez való hozzáférést, ide számítva az egészségügyi nyilvántartásokat, a jogosítványkérelmeket és -megújításokat, és más közösségi programokat is… a Huawei… gyártmányai teszik lehetővé az autósok számára a szabad parkolóhelyek megtalálását… A rendszer nagyon megkönnyíti a betegek és a kórházak számára a releváns nyilvántartások elérését…”[53] *A kiépülő rendszer tökéletes példája lehet az előző fejezetben elérni kívánt állami működésnek, vagyis az olyan szolgáltató államnak, amely képes jóléti intézményeit átemelni a digitális környezetbe, sőt fokozni is képes ezáltal azokat. Azonban ott van egy hatalmas „de” a mondat végén, hiszen e rendszerek révén nem csupán erre képes Kína, hanem az emberek nyomon követésére, osztályozására és adataik tényleges birtoklására is.*[54] Érdemes eme megoldásoknál kicsit elidőzni. A kínai Aranypajzs projekt, ahogy arra a Freedom House 2020-as internetszabadságról szóló jelentése felhívja a figyelmet, a glóbusz legmodernebb és legösszetettebb rendszere. Nagy hangsúly helyeződött arra, hogy ez egy összetett rendszer, mivel már nem csupán a kibertéri tevékenységet figyeli és korlátozza, hanem számos rendszert kapcsol össze. Így a közterekre, az otthonokba, munkahelyekre, de mint fentebb láttuk, már az általános iskolákba vagy óvódákba telepített megfigyelőkamerákat, a Covid19 terjedését megakadályozandó

geopolitikai jelentőségét. Lásd Engel Péter: A Bundeskartellamt Facebook-döntése – az adatgyűjtés versenyjogi kockázatai. *Verseny Tükör*, 2019/1. szám, 70–76. o.; Gellén Klára: Tisztességtelen kereskedelmi gyakorlatok az online térben – fókuszban a közösségi média. *In Medias Res*, 2020/1. szám, 127–140. o.; Farkas Ádám: Biztonság – Geopolitika – Digitalizáció, avagy Amaël Cattaruzza „A digitális adatok geopolitikája” című kötetének főbb üzenetei. *SmartLaw Research Group Working Paper*, 2021/1. szám, 1–13. o.

[53] Mosco: i. m. (2019) 111–112. o.

[54] Kollár Csaba: Kína és a társadalmi kredit rendszere. *Hadtudomány*, 2020/2. szám, 79–97. o.

hőérzékelési rendszereket, egészségügyi állapottal és kontaktkutatással kapcsolatos applikációkat, valamint a big data-alapú elemző rendszereket, az online tevékenységet korlátozó algoritmusokat és természetesen az arcfelismerést szolgáló technológiákat.[55] Nem lehet megfeledkezni a Kínai Nagy Tűzfalról sem, amely a külső tartalmak elérhetetlenné tételét szavatolja, míg az állami cenzúrát e közegben maga a Pajzs teszi lehetővé. Ennek köszönhetően egyre nagyobb terjedelmében teremtődik meg az alapja a társadalmi kreditrendszernek, ami politikai és társadalmi status quo rögzülését eredményezi, ahol csak az lehet a társadalom hasznos tagja, és csak az léphet előre, aki megfelelően teljesít a pontok/kreditek rendszerében.[56] Gosztonyi Gergely felhívja arra a figyelmet, hogy ez a jelenség nem példa nélküli, és egyre több követőre talál. „Nyilvánvalóan nem lehet társadalmi, szociális vagy akár politikai helyzet kapcsán egy kalap és egy szabályozási modell alá helyezni az összes ázsiai országot, az mégis látható, hogy – az eltérések ellenére – az internet szabályozásával és a tartalomszabályozással kapcsolatos felelősségi kérdésekben egy sokkal szigorúbb utat választottak, mint Európa vagy az Amerikai Egyesült Államok… A fő cél természetesen politikai: megakadályozni, hogy az online világban olyan gondolatok terjedjenek, amelyek esetlegesen politikai ellenállást szülhetnének a való életben."[57] Ahogy Gosztonyi is kifejti, ez nem egy homogén csoportja az államoknak, azonban egyre nyilvánvalóbbá válik, hogy egyre több állam választja annak a lehetőségét, hogy a polgárait kibertérben vagy kapcsolódó eszközök révén „kordában" tartsa, az internetét pedig a lehető legteljesebb mértékig kontrollálja.

Szingapúr is hasonló példát mutat Okos Nemzet projektjével, amely felhasználásával „kezdetektől fogva tervezték… egy centralizált műveleti központ létrehozását, a polgárokról és a látogatókról összegyűjtendő nagy mennyiségű adat kezelésére…", ez pedig lehetővé teszi „az átfogó megfigyelést és az egyének magatartásának szigorú szabályozását".[58] A megvalósítás hivatalos céljai között szerepel a betegségek terjedésének gyorsabb feltérképezése vagy a terrorista támadásokra való gyorsabb reagálás lehetősége. Megvalósításán fúzióban dolgoznak az állami intézmények és a magánszféra vállalatai, akárcsak Kína esetében. A rendszerek kialakításában és üzemeltetésében történő közreműködésért cserébe a kormányzat „megosztja az adatokat a gazdaságfejlesztés és a kereskedelmi sikerek ösztönzése céljából"[59]. Két szereplő, vagyis az állam és a technológiai vállalatok együttesen érdekeltté válnak a status quo fenntartásában, hiszen egyfelől totális felügyelet alá helyezték az egyéne-

[55] *Freedom on the Net 2020 – The Pandemic's Digital Shadow.* Freedom House (https://freedomhouse.org/sites/default/files/2020-10/10122020_FOTN2020_Complete_Report_FINAL.pdf) 21. o.

[56] Szikszai Marcel: Disztópia Kínában? Tanulmány a társadalmi kreditrendszer a kínai jogfejlődés tükrében. *Infokommunikáció és Jog,* 2020/1. szám, 21–26. o.

[57] Gosztonyi Gergely: *Cenzúra Arisztotelésztől a Facebookig – A közösségi média tartalomszabályozási gyakorlatának komplexitása.* Budapest, Gondolat Kiadó, 2022, 157, 165. o.

[58] Mosco: i. m. (2019) 109. o.

[59] Mosco: i. m. (2019) 110. o.

ket, másfelől a gazdasági fejlődés folyamatos fenntartását teszik lehetővé az állami megrendelések, harmadsorban a meglévő adatok birtokában a gazdasági szféra is meg tudja hozni a szükséges intézkedéseket, stratégiát a profit folyamatos növelése érdekében. Mit nyer ezzel a felhasználó? Javuló közszolgáltatásokat a szabadságáért cserébe, de lényegében a választás lehetősége egy másodpercig sincs biztosítva a részükre. Ilyen város kialakítását tűzte ki célul az Egyesült Arab Emirátus Dubaj esetében, de ezt látjuk Rio de Janeiróban, Malajzia és Fülöp-szigetek jelentősebb városaiban, valamint India is meghirdette ezen programját All India City Challenge néven, amelynek alakításába azonban a helyi közösségek aktívan bele kívánnak szólni.

A rendszert a saját internet létrehozása és annak totális felügyelete tette teljessé, mint a kínai Aranypajzs rendszer, vagy az orosz internet,[60] *ezzel ezen államalakulatok képesek szinte totális ellenőrzés alatt tartani saját polgáraikat, hiszen minden olyan tartalmat tudnak blokkolni, amely az államhatalom szempontjából nem kívánatos.* Ezen megoldás az okosváros-projektekhez hasonlóan szintén követőkre talált. Irán közvetlenül kínai know-how felhasználásával kíván „halal"[61] internetet kiépíteni, amelyet Zambia is követ a kritikus tartalmak blokkolása területén. Emellett a kormányellenes, kormánykritikus hangok blokkolása is bevett gyakorlattá vált a közösségimédia-felületeken, ezt alkalmazza Kuba, Nigéria, Kolumbia, Banglades, Szenegál, illetve a teljes internet elérhetőségét megakadályozva a Kongói Köztársaság, Csád, Örményország vagy Mianmar.[62] Ezen államok fellépésének az alapja, a korábban Kína vagy Oroszország által megfogalmazott elv: a szuverén internet elve, amely szerint minden állam szabadon rendelkezik a hozzá tartozó kibertér felett, ebbe más állam nem avatkozhat be, ott szabadon határozhatja meg az elérhető tartalmakat, azokhoz való hozzáférést. A Freedom House fent már említett jelentése erre kitérve rámutat, hogy Kína és Irán a leginkább zárt saját internet tekintetében, de ehhez a táborhoz közelít Oroszország, Törökország és Vietnám is,[63] a tábor pedig folyamatosan bővül.

Az elmúlt években az is világossá vált, hogy az államok a technológia újdonságait legalább ilyen, aktív módon használják más államokkal szemben is. A hibrid konfliktusok eszközparkjába beemelt kibertéri műveletek rendkívül széles tárházát adják a szemben álló állam egyes rendszereinek támadására. Folyamatos fenyegetést jelentenek a dez-

[60] Gosztonyi, Gergely: Special Models of Internet and Content Regulation on China and Russia. *ELTE Law Journal*, 2021/2. szám, 87–99. o.

[61] A halal fogalom az iszlám vallásban fontos értéket képvisel, jelentése megengedett vagy tiszta. Az iszlám jog szerint minden tevékenység megfelel a halalnak, amely megengedett, és az előírásoknak, dogmáknak megfelel. Ennek felhasználásával kontrollált internetes információáramlást nevezhetjük halal internetnek. Lásd Iran creates „Halal Internet" to control online information. *RSF – Reporters without Borders*. 2016. szeptember (https://rsf.org/en/news/iran-creates-halal-internet-control-online-information).

[62] Gosztonyi: i. m. (2021) 97–98. o.

[63] Freedom House, 2. o.

információs kampányok, amelyek érdemben az államalakulatok mindegyikével szemben alkalmazhatóak. Az oroszok folyamatos dezinformációs tevékenysége figyelhető meg az elmúlt évtizedben. Ennek során beavatkoztak a 2016-os amerikai elnökválasztásba, akár álhírek terjesztésével, akár a szemben álló jelöltekkel kapcsolatos kompromittáló információk kiszivárogtatásával, vagy a közösségimédia-platformokon keresztül megfelelően időzített hírcsomagokat juttattak el felhasználókhoz.[64] A francia sárgamellényes tüntetés időszakában hamis híreket terjesztettek német, spanyol, holland, lengyel, svéd és olasz nyelven. Az RT orosz állami hírcsatorna néhány riportere részt vett a tüntetéseken, és úgy ábrázolta a helyzetet, mintha Párizs háborús övezet volna. A dezinformációs kampányból nem maradhatott ki a hagyományos média munkatársainak lejáratása sem, őket korruptnak, megbízhatatlannak, a kormánnyal mindenben összejátszónak mutatták be.[65] A legyártott és azonosított száz álhírt több mint 4,1 millióan osztották meg, és 105 millióan tekintették meg.[66] De mindkét állam rendkívül erős dezinformációs kampányt folytatott a Covid19 járvánnyal és nyugati vakcinák hatékonyságával kapcsolatban, ezzel is nehezítve a térség járvány elleni védekezését.[67] Jelenleg zajló orosz–ukrán háború is élesen rávilágít erre a problémakörre. A háború szinte vagy inkább láttatni kívánt szinte minden pillanatát követni tudjuk a közösségi média felületein.[68] Ennek célja mindkét oldalról, hogy a hadviselő felek megfelelően tudják tálalni érdekeiket saját, illetve a világ más társadalmai irányába, vagyis mindkét oldal él a dezinformáció eszközével.[69] Földi László biztonságpolitikus ezt a következőképpen foglalta össze: „Nagyon álságos ez a helyzet, a közvéleményt afelé tolják, hogy tendenciózusan döntsünk, miközben gyakorlatilag kihúzzák a lábunk alól azt a lehetőséget, hogy objektívek maradjunk… megjegyezve, hogy az egyik fél amerikai, a másik fél pedig orosz propagandáról beszél, miközben valójában mindkét hatalomnak megvannak a maga eszközei a befolyásolásra."[70]

[64] Lina Rosenstedt: Improving Cooperation with Social Media Companies to Counter Electoral Interference. *Hybrid Coe Paper*, 2021/5. szám, 5. o.

[65] Jarmo Makela: Countering Disinformation: News Media and Legal Resilience. *Hybrid CoE Paper,* 2019/1. szám, 10–13. o.

[66] *Yellow Vests Flooded by Fake News – Over 100M Views of Disinformation on Facebook. Avaaz Report.* 15. 03. 2019. (https://avaazimages.avaaz.org/Report%20Yellow%20Vests%20FINAL.pdf).

[67] Ben Dubow – Edward Lucas – Jake Morris: *Jabbed in the Back: Mapping Russian and Chinese Information Operations During Covid-19.* The Center for European Polidy Analysis (CEPA), 2020.

[68] Pató Viktória Lila: *A háború hatása a közösségi médiára.* Nemzeti Közszolgálati Egyetem Európai Stratégia Kutatóintézet (https://eustrat.uni-nke.hu/hirek/2022/03/01/a-haboru-hatasa-a-kozossegi-mediara).

[69] Huszák Dániel: Példátlan információs háború zajlik Ukrajna körül – Elképesztő mennyiségű hazugság ömlik a világra. *Portfolio* (https://www.portfolio.hu/global/20220226/peldatlan-informacios-haboru-zajlik-ukrajna-korul-elkepeszto-mennyisegu-hazugsag-omlik-a-vilagra-529377).

[70] Holló Bettina: Földi László a háborúról: Állásfoglalásra késztetnek, de az igazság magjától is eltántoríthatnak. *Index* (https://index.hu/belfold/2022/03/06/haboru-ukrajna-alhirek-biztonsagpolitika-foldi-laszlo-demko-attila/).

Legalább ilyen jelentős a különböző intenzitású kibertámadások elkövetése akár civil, gazdasági célpontok ellen,[71] akár állami intézmények rovására. Ezek közül legismertebb a 2007-es Észtországot és a 2008-as Grúziát ért támadás,[72] azonban ezenfelül számos kisebb volumenű szcenáriót tudunk feljegyezni az elmúlt évtizedből. Ilyennek tekinthetjük az Észak-Koreához köthető WannaCry zsarolóvírus támadást is, amely jelentős károkat okozott több államnak, gazdasági szereplőnek.[73] Az okozott anyagi károk mértékét már felvázoltuk a korábbi fejezetekben, annyit érdemes ismét felvillantani, hogy az elkövetkező években a kiberbűncselekmények által okozott kár mértéke, jelenleg 6,9 billió dollár,[74] a Cybersecurity Ventures becslései szerint ez 2025-re 10,5 billió dollár lesz, ami megközelítőleg az Európai Unió vagy Kína éves nominális GDP-jének az összege.[75] Szintén megfigyelhető ennek az eszköznek az alkalmazása a jelenleg zajló orosz–ukrán háborúban is, amikor az orosz haderő legalább annyira aktív a kibertérben, mint a hagyományos hadviselés területén.[76] *Ezzel kapcsolatban érdemes leszögezni, hogy a kibertér nem hozott létre önmagában új konfliktuskategóriákat, nem eredményezett a korábbitól ismeretlen hadviselési metódusokat, hanem ez valójában a hadiviselés korábbi eszköztárának a fejlesztését jelentette: a hatékonyság és az erő sokszorozását, műveleti képességek fokozását.*[77] Az orosz–ukrán konfliktus korábbi szcenáriói is visszatükrözik ezt. A West Point-i katonai szakértők szerint az oroszok szinte példa nélküli módon egymást kiegészítve,

[71] „A 2020-as évben pusztító útjára indult Covid–19 járvány az informatikai biztonság területén is kifejtette hatását – globális szinten jelentősen megnövekedett a kibertámadások száma. A Kaspersky felmérése szerint »az Európai Unióban az internetet használó számítógépek 13,7 százalékán tapasztaltak legalább egy böngészőalapú, rosszindulatú programtámadást«, (és a támadások számát tekintve) »az első tíz között találjuk Magyarországot is«. Nagyságrendileg ugyan az otthoni gépek vannak leginkább kitéve kémkedésnek, adatlopásoknak, rongálásnak és egyéb támadásoknak, de céges környezetben a statisztikák nem kevésbé lesújtóak. Az amerikai CSI egy korábbi felmérése szerint a válaszadók 85%-a észlelt már számítógépes betörési kísérleteket az adott naptári évben, sőt, 64% esetében ez anyagi veszteséget is jelentett." Németh Richárd: A kibertérből érkező fenyegetések elleni védekezés vállalati környezetben. *GIKOF Journal*, 2021, 48. o.

[72] Kelemen Roland – Pataki Márta: A kibertámadások nemzetközi jogi értékelése. *Katonai Jogi és Hadijogi Szemle*, 2015/1. szám, 53–90. o.

[73] *North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions*. Department of Justice, 2018. szeptember 6. (https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and).

[74] *Federal Bureau of Investigation Internet Crime Report 2021*. Internet Crime Complaint Center (https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf), 7. o.

[75] Steve Morgan: *2019 Official Annual Cybercrime Report – Cybercriminal activity is one of the biggest challenges that humanity will face in the next two decades.* (https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf).

[76] Joe Tidy: Ukraine crisis: ‚Wiper' discovered in latest cyber-attacks. *BBC News*, 2022. 02. 24. (https://www.bbc.com/news/technology-60500618).

[77] Sascha-Dominik Bachmann – Hakan Gunneriusson: Hybrid Wars: The 21st Century's New Threats to Global Peace and Security. *South African Journal of Military Studies*, 2015/1. szám, 82. o.

kombinálva alkalmazzák a kiberhadviselés, az elektronikus hadviselés és az információ műveletek eszközparkját.[78] Ahogy ezt Kiss Álmos Péter kifejtette: „az oroszok egyáltalán nem osztják fel az információs teret. Nincs különálló kibertér, nem tesznek különbséget a számítógép-hálózatokat érintő műveletek és más információszerző, információfeldolgozó és információáramlást zavaró tevékenység között. Az orosz információs hadviselés harctere tehát a teljes kognitív tartomány."[79] *Látható, hogy a kibertéri eszközpark beépült a haderő tevékenységébe, legyen az akár befolyásolás, akár hírszerzés, akár támadó eszköz, amely így a békeidős összhaderőnemi felkészítésnek, majd pedig eszközparkjának immanens részét képezi. Így lehetséges az, hogy a hagyományos háborúnak is vannak – lásd orosz–ukrán – hibrid szcenáriói.*

A kibertér a fentieken túl lehetőséget biztosít a szakadár és terrorista csoportok anyagi támogatására, szervezésére, amelyek így képesek lehetnek későbbi akciókhoz kapcsolódó információszerzésre, az ilyen akciók kibertéri támogatására, az akciók kibertéri előkészítésére és adott esetben – ahogy Lewis fogalmazott[80] – a közlekedési hálózatokkal, finomítókkal, gátakkal, katonai létesítményekkel, kórházakkal, bankokkal, kormányzati intézményekkel stb. szembeni támadás lefolytatására. Az oroszok rendkívül sikeresek voltak az ukránok elleni hibrid konfliktus során, hiszen tökéletesen tudták alkalmazni a korábbi évtizedek tapasztalatait és kapcsolati hálóját.[81]

A kibertér és a hozzá tapadó technológiai újdonságok pozitív hozadékai mellett olyan, az államok biztonságát, biztonsági környezetét befolyásoló természettel bír, amely így számos ponton tépázza meg az 1945 utáni nemzetközi jogi rezsimet, sok esetben feloldva azt a napi politikai realitások folyamában. A kibertérben alkalmazott vagy támogatott hadászati eszközök nem újak, azonban a korábbi eszközöket a végletekig tudják fokozni, eredményesebbé és hatékonyabbá tenni. Jól bizonyítják ezt a hibrid konfliktusok, kiemelten az ISIS tényekedése, valamint 2014-től az oroszok ukrajnai tevékenysége volt az egyik mintapéldánya ennek a hadviselésnek, amelynek magasabb fokozatba kapcsolását jelenti a 2022 februárjában kirobbant nyílt háború. A korábbi szcenáriók esetében is már egyértelművé vált, hogy a technológiai újításokat alkalmazva, egyre fokozottabb mértékben kezdődött meg az ENSZ Alapokmányban lefektetett erőszak általános tilalmának eróziója. Főként

[78] Aar Aaron F. Brantly – Nerea M. Cal – Devlin P. Winkelstein: *Defending the Borderland – Ukrainian Military Experiences with IO, Cyber, and EW.* Army Cyber Institute at West Point, West Point, 2017 24. o.

[79] Kiss Álmos Péter: A hibrid hadviselés természetrajza. *Honvédségi Szemle*, 2019/4. szám, 31. o.

[80] James A. Lewis: Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats, *Center for Strategic and International Studies*, 2002 (https://www.steptoe.com/images/content/4/5/v1/4586/231a.pdf).

[81] Káncz Csaba: Az orosz titkosszolgálatok és a szervezett bűnözés ijesztő kapcsolatrendszere. *privátbankár.hu*, 2021. (https://privatbankar.hu/cikkek/makro/az-orosz-titkosszolgalatok-es-a-szervezett-bunozes-ijeszto-kapcsolatrendszere.html).

annak köszönhetően, hogy a polgári és kombattáns elkülönítése a harcászat nem klasszikus terepén szinte lehetetlenné vált, így a betudhatóság korábban kiforrott és többnyire a felek által betartott szabályait nem vagy csak nagyon nehézkesen lehet alkalmazni. Az ukrán háború rávilágított arra is, hogy a népek önrendelkezése és külső állam beavatkozásától mentes létezése is feloldódni látszik a nagyhatalmi törekvésekben, amelyeket akár későbbi nemzetközi szerződésekkel is megerősítenek,[82] illetve végső esetben nagyhatalmi deklarációkkal legitimálnak.[83] A háború és béke határa elmosódott az elmúlt években, a legtöbb konfliktus esetében nem tudjuk, hogy az „éppen még" vagy az „éppen már" állapotában vagyunk. Erre szintén rávilágított az orosz–ukrán válság, hiszen a tényleges harci cselekmények a felek között már jóval a 2022-es inváziót megelőzően megindultak.

Ezek összessége eredményezi a biztonság és védelem újradefiniálását, a totális biztonság irányába történő elmozdulást.[84] A nemzetközi közösség államainak egyik pólusa már megtette ezt, és ezen államalakulatok – főként a kibertér révén – már sokkal közelebb helyezkednek a warfare state államához, amely saját biztonságának szavatolását csak a hatalom révén, az erő által látja biztosítottnak.[85] Ezen államokban a haderő folyamatos erősítése mára létérdekké vált, a politikai hatalom, haderő és gazdaság hármasa egyetlen érdeket szolgál: a status quo-minimum fenntartását, vagy még inkább a hatalmi szféra kiterjesztését.

2. CYBERFARE STATE MODELLJEI

Stumpf István az *Erős állam – alkotmányos korlátok* című könyvében felhívja a figyelmet arra, hogy az államnak vannak olyan alapvető, nélkülözhetetlen funkciói, amelyeket mindenképpen el kell látnia. „Nincs olyan más, a legitim erőszak monopóliumával felvértezett intézmény, amely a szervezett közösségi együtteléshez nélkülözhetetlen alapfeltételeket az államot helyettesítve biztosítani tudja."[86] Ezen alapfunkciók első köre között tartja számon a joguralom, a magántulajdon biztosítását (belbiztonság), valamint a honvédelmet, vagyis a külső biztonságot.

[82] Lásd a minszki szerződéseket az ukrán konfliktusban. Lásd bővebben: Póti László: Minszk–2 után két évvel: Hol tart a békefolyamat? *KKI Elemzések*, 2017/5. szám.

[83] Vlagyimir Putyin elismerte a két szakadár népköztársaságot. *hirado.hu*, 2022. 02. 22.

[84] Farkas Ádám: Gondolatok a totalitás 21. századi esszenciájához. In Pongrácz Alex (szerk.): *Ünnepi tanulmányok a 65 éves Cs. Kiss Lajos tiszteletére. Út vocatio scientia.* Budapest, Ludovika Egyetemi Kiadó, 2021, 65–80. o.

[85] Fred J. Cook: The Warfare State. *The Annals of the American Academy of Political and Social Scince*, 1964/1. szám, 102–109. o.; Keith L. Nelson: The Warfare State: History of Concept. *Pacific Historical Review,* 1971/2. szám, 127–143. o.; David Edgerton: *Warfare State – Britain, 1920–1970.* Cambridge, Cambridge University Press, 2006, 59–107. o.

[86] Stumpf István: Új államalapítás? Alkotmányos és kormányzati kihívások. In Stumpf István (szerk.): *Erős állam – alkotmányos korlátok*. Budapest, Századvég Kiadó, 2014, 27. o.

Az előző fejezetek érzékeltetik, hogy a kibertér oly mértékben alakította át a társadalmi totalitás, azon belül az egyén életét és hatófokát, a társadalmi hálózatokat, az állam működését, valamint a biztonsági – természetesen a hagyományos térhez kapcsolódó egyéb kihívások sem felejtendők el ebben körben[87] – környezetet, hogy az államok több esetben, igaz, leggyakrabban csak átmenetileg, a korábbi mércéhez képest kisebb terrénumban tudnak megfelelni ezeknek a követelményeknek. Márpedig, ha „a társadalmi félelemek eszkalálódnak… Ez egy negatív spirált eredményez. Minél inkább teszik ezt, annál nagyobb a zűrzavar és az erőszak, és minél nagyobb a zűrzavar és az erőszak, annál kevésbé képesek az államok a helyzet kezelésére, következésképp annál több ember vonja meg a bizalmát az államtól…"[88] Azaz a közrendbe és azt szavatoló katonai karakterű szervekbe vetett bizalom elvesztése annulálná a biztonságot, ezáltal felszámolná a normál állapotot.

Az államok mára a kibertér jelentette lehetőségeket és kihívásokat tökéletesen érzékelik (nem véletlen például, hogy a NATO a kiberteret hadszíntérré minősítette), azok biztonságot érintő hatására megpróbálnak választ adni. Azonban ezt a választ az egyes államok történeti és társadalmi hagyományai, valamint politikai és állam- és jogtudományi tradíciói, nagyhatalmi törekvései erősen befolyásolják. A kibertér biztonsága szempontjából az egyik fő ágens az egyén, akár passzív, akár aktív szereplőként figyelünk rá, mely az előző fejezetekben látható módon soha nem látott mértékben tud hatni a nemzet biztonságára. Nem véletlen, hogy a tradíciók, politikai rendszerek mentén az egyén szerepére történő reagálás az egyik legfontosabb választóvonal a vizsgált államok között. Ennek köszönhetően két modellértékű rendszer alakult ki. Az egyik modell a jogállami keretek között gondolkodó államok halmaza, míg a másik, a kibertérben és kapcsolódó eszközökben lehetőséget látó és kihasználó, a társadalmának lehető legteljesebb ellenőrzésére törekvő államok foglalata. Természetesen a két halmaz egyike sem homogén, azokon belül eltérő mértékben valósul meg egyik oldalról a technológiai rendszerekre épülő totális kontroll, míg a másik halmaz államai között sem azonos mértékben veszik figyelembe a jogállami paradigma egyes pilléreit. Ennek ellenére érdemes elkülöníteni ezeket a modelleket, és alapjaiban elemezni azokat.

[87] Juhász István – Petruska Ferenc: A védelmi-biztonsági szabályozási reformot indukáló biztonsági környezet-változás elemeinek beazonosítása, szakmai értékelése. *Védelmi-biztonsági Szabályozási és Kormányzástani Kutatóműhely,* 2022/32. szám, 4–46. o.

[88] Szigeti Péter: Vázlat a közbiztonság három dimenziójáról: világrendszer – nemzetállami szint és lokalitás. In Szigeti Péter: *A valóság vonzásában – Jogelméleti* és *Jogtudományi Közlöny,* Győr, ELTE–SZIF ÁJK, 2001. (https://mek.oszk.hu/04200/04241/04241.htm#16).

2.1. A smart total control cyberfare state

Az előző fejezet rámutatott arra, hogy az államok egy köre a technológiai fejlesztések révén nemcsak a jóléti funkciókat erősíti a kibertérhez kötődő eszközök révén, hanem a lehető legteljesebb kontrollra törekszik polgárai felett. Az is látható volt, hogy ennek a gondolkodásnak az alapja a szuverén[89] internet elvének vagy kiberszuverenitásnak a megalkotása, amely körben minden állam rendelkezik saját, lehatárolható kibertérrel, amelybe nyilvánvalóan a hagyományos térben tapasztalható állami szabályozási, rendészeti és védelmi attitűdjét ülteti át.[90]

Adam Segal neves amerikai kiberbiztonsági szakértő rávilágít arra, hogy a kiberszuverenitás eszméjét Kína igen nagy mértékben azért fogalmazza meg és kívánja lehető legteljesebben kialakítani, mert e területen is globális hatalmi pozícióra tör, így az sem meglepő, hogy e koncepciónak egy belső és egy külső aspektusa van. Azonban nem feltétlenül ez az indoka annak, hogy a tézis elfogadottabbá válik, hanem az, hogy egyre több államnak okoz jelentős problémát a dezinformáció, a magánéletet és magántulajdont fenyegető veszélyek, a gazdasági hozadékai a kiberbűncselekményeknek, és nem utolsósorban sok állam visszásnak tekinti a nagy technológiai vállalkozások hatalmi koncentrációját, amely a szabályozatlan vagy alulszabályozott kibertérből ered. Azonban egy ilyen rendszer működtetéséhez megfelelő gazdasági és technológiai kapacitás is szükséges, mivel az elv kimondása önmagában nem fogja létrehozni a technológiai hátteret, és azt fejleszteni, működtetni, így az jelentős gazdasági forrással jár.[91] Kína mindezt sikeresen tudta kivitelezni, így a Kínai kiberdiplomáciának egyértelmű és működő elvi alapja a kiberszuverenitás.[92] A modell egyértelműen követőkre talált azon államok között, amelyek hajlamosak amúgy is a kibertér elérésének korlátozására, illetve osztják a fenti aggályokat, és Kína globális törekvései nyomán hajlandó is megosztani azt. Nem véletlen, hogy a kínai know-how átvételét láthatjuk, vagy arra való törekvést Etiópiában, Egyiptomban, Jordá-

[89] Szuverenitás fogalmáról lásd bővebben: Horváth Barna: *Angol jogelmélet.* Budapest, A Magyar Tudományos Akadémia Kiadása, 1943; Pongrácz Alex: Szuverenitás és alkotmányosság a globális erőtérben. *Pro Publico Bono,* 2016/1. szám, 108–119. o.; Pongrácz Alex: Mozaikok a magyar szuverenitásfelfogás történetéből. In Karácsony András (szerk.): *Szuverenitáskérdések. Elméletek, történetek.* Budapest, Gondolat Kiadó, 2020, 98–113. o.

[90] Gosztonyi Gergely: A kínai internetcenzúra modellje. *Pro Futuro,* 2022/1. szám, 7–8. o.

[91] Adam Segal: China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace. In Nadége Rolland (szerk.): *An Emerging China-Centric Order – China's Vision for a New World Order in Practice.* Seattle, The National Bureau of Asian Research, 2020, 86. o.

[92] Molnár Dóra: Nagyhatalmi kiberdiplomácia – az Egyesült Államok, Kína és Oroszország a nemzetközi kiberporondon. In Török Bernát (szerk.): *Információ- és kiberbiztonság.* Budapest, Ludovika Egyetemi Kiadó, 2020, 357–371. o.; Gosztonyi Gergely: Az internet-hozzáférés korlátozásának gyakorlata az Emberi Jogok Európai Bírósága előtt. *In Medias Res,* 2021/1. szám, 91–101. o.; Gosztonyi Gergely: Special Models of Internet and Content Regulation on China and Russia. *ELTE Law Journal,* 2021/2. szám, 87–99. o.

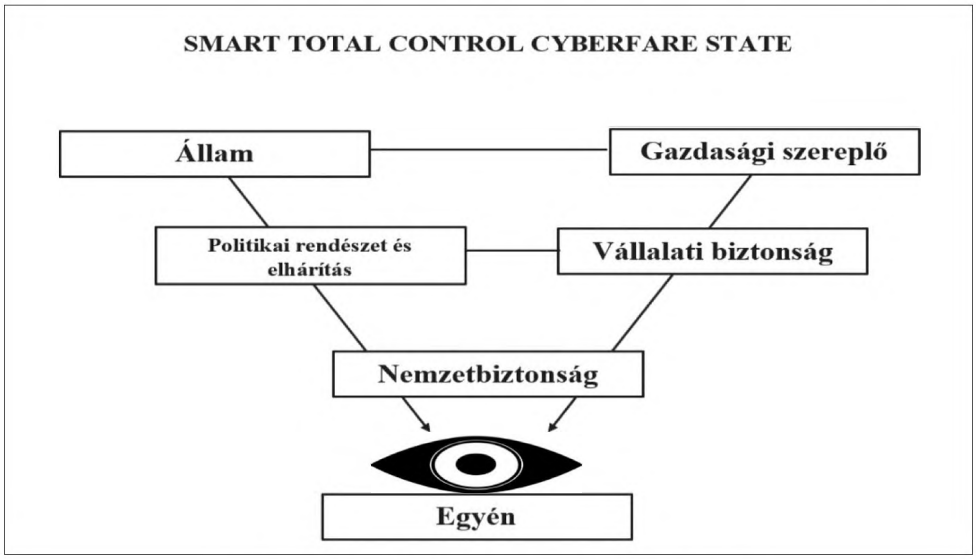
niában, Libanonban, Líbiában, Marokkóban, Szaúd-Arábiában, az Egyesült Arab Emírségekben. De ez nem csupán a technológia- és az intézményrendszerben ölt testet, hanem a jogi szabályozás másolásában is. Tanzánia Kínáéhoz hasonló kiberbiztonsági törvényt fogadott el. Egyiptom, Laosz, Pakisztán, Uganda, Vietnám és Zimbabwe olyan törvényt fogadott el, amely kínai mintára lehetővé tette a weboldalak blokkolását, a valós név regisztrációját, az adatmegosztást és a tartalom eltávolítását.[93] Tehát Kína valós és működő alternatívát kínál mind szabályozás, mind technológiai vívmányok tekintetében. Tőle részben függetlenül, de ezen az úton jár Észak-Korea, Oroszország és Irán is. Ha nem is ekkora terrénumban, de lépéseket tett ebbe az irányba Törökország, Szingapúr is. Tehát azt kell mondani egyértelműen modellértékű a kínai kiberszuverenitás-felfogás, és nemcsak technológiai oldalról, hanem jogi, valamint szervezeti rezsim esetében is.

A kibertér és az ahhoz kapcsolódó rendszerek ilyen rendkívül sikeres – még ha európai szemmel nézve rendkívül visszás – kiaknázása, felhasználása és alkalmazása, amely főként Kínában vagy Oroszországban, Szingapúrban, illetve akár egyes aspektusokban Észak-Koreában figyelhető meg – de mint láttuk, emellett számos követő államra talált legalább részmegoldásaiban – megteremtette a cyberfare state hatalmi államon nyugvó almodelljét. Ennek keretében az állam a birtokolt erőhatalom révén ténylegesen vagy jelentős terrénumában létrehozza a saját szuverén kiberterét, azt a lehető legteljesebb egészében birtokolja, ellenőrzi, az ettől elkülönült külső kibertérben megjelenő államok technikai, szabályozási, védelmi hiányosságait kihasználva pedig soha nem látható eredményességgel tudja befolyásolni, eszkalálni más társadalmak töréspontjait, illetve tudja megbénítani egyes alrendszereit. Mindezeket anélkül, hogy legtöbb esetben ténylegesen fegyveresen konfrontálódna a megtámadott állammal.

Ezt a rendszert azért működtetik, a tevékenységet azért valósítják meg, mert a kialakult új biztonsági környezetben meglátásuk szerint a totális felügyelet és totális „erőszak-monopólium a béke és a kiszámítható rend legfőbb biztosítéka"[94]. Ennek kialakításában pedig – mint láttuk – fúzióban tevékenykednek, működnek és fejlesztenek az egyes államok és gazdasági szereplőik. Az egyén ezekben az államokban a lehető legteljesebb kontroll alatt éli hétköznapjait, lényegében kizárólag egyes részobjektumok üzemeltetője (munkája révén) és fogyasztója a rendszer által engedett és kínált szolgálatásoknak, de valódi döntéssel nem rendelkezik adatvagyona felett sem. Ebben a közegben tehát az állam hatékony működését, biztonságának szavatolását az állam és a gazdasági szereplők összefonódása, érdekközössége teremti meg, ahol e közös cél érdekében az egyént mint a (kiber)biztonság legtörékenyebb lánc-

[93] Segal: i. m. (2020) 94–95. o.

[94] Pongrácz Alex: A politika folytatása más eszközökkel? Avagy gondolatok az állam és az erőszak kérdésköréről. *Államtudományi Műhelytanulmányok*, 2017/17. szám, 9. o.



Smart total control cyberfare state (saját szerkesztés)

szemét[95] megpróbálják kivonni, szerepét a lehető legcsekélyebb mértékűvé tenni, ennek pedig eszköze a személye feletti totális kontroll és adatai feletti állami és gazdasági rendelkezés totalitása.

Ezen államok (kiber)biztonság szavatolását jelentő legjobb gyakorlat kialakítása, folyamatos nyomkövetése és szükséges korrekciója az állam és az ebben érintett gazdasági szereplők közös érdeke és együttműködésük gyümölcse, amelyben az egyén nem érdekeltként, hanem kizárólag irányított, kontrollált erőforrásként jelenik meg. Ebben a legjobb gyakorlatban a kibertérre támaszkodó technológiai újításokon nyugvó szociális, jóléti intézményeket, végső soron a szolgáltató közigazgatás javítását, modernizálását társítják a totális kontroll és adatok feletti totális rendelkezés lehetőségével, amelyekhez sok esetben támadó potenciál kiépítése kapcsolódik. A cyberfare state ezen hatalmi jellegű attribútumokat felmutató államait a fentiek okán smart total control cyberfare statenek nevezhetjük.

2.2. A totális biztonság és védelem (jog)állami adaptációjának a lehetősége

Ezzel szemben a nyugati államoknak a saját cyberfare state modelljük kialakítása során teljesen más alapokról kellett, kell indulniuk. A digitalizáció jóléti reformját már megkezdték a 2000-es évek elején, és ebben, ha nem is minden területen, de lát-

[95] Informatikai szempontból lásd Németh Richárd: Kiberfenyegetettség nagyvállalati környezetben. *Magyar Bűnüldöző*, 2020/2. szám, 23–41. o.

ványos sikereket értek el. Az előző fejezetben látható volt, hogy sikerrel alakították át a szolgáltató közigazgatást, nagy volumenű innováció jelent meg többek között az oktatás, kutatás, egészségügy területén, emellett rendkívül sikeres okosváros-programok[96] is futnak, de az önvezető járművekkel kapcsolatos projektek[97] vagy az MI programok[98] is számos előnnyel kecsegtetnek. Azonban itt is jelentős eltéréseket lehet kimutatni a másik pólus államaihoz képest, ugyanis ebben kulcsfontosságú, sőt élenjáró szereplők voltak a technológiai óriásvállalatok, azonban – szemben például Kínával – ez nem jelentette az állam és a gazdasági szereplők fuzionális összefonódását, ellenben sok esetben jelentős érdekellentétek alakultak ki, ami adódik a piacok struktúrájából, az állam és gazdasági szereplők közötti kapitalista államfelfogás tradicionális ellentéteiből.[99] Szintén teljesen más képet mutat az egyéni adatok kezelhetősége ezen államok esetében. Sok esetben a transznacionális vállalatok gazdasági érdekeik fokozott érvényesítése érdekében a kezelt adatokkal visszaéltek, amely bár jelentős bírságot eredményezett, azonban gazdasági helyzetükben, társadalomban betöltött szerepükben ez nem jelentett változást. Itt az állam vagy azok közössége próbál egyre szigorúbb szabályokat alkotni.[100] Másik oldalról az állam, a biztonsági környezet átalakulása miatt, próbálja a nemzetbiztonság sebezhetőségét csökkenteni, és az ehhez kapcsolódó információéhséget csillapítani. Ez pedig ellentétes a gazdasági és az egyéni szereplők érdekeivel, emellett az alkotmányosan körülhatárolt állami működés miatt jelentős akadályokba ütközik, melyet sok esetben hangos ellenkezés, nemzetközi bírói fórumok előtti fellépés követett.[101] *Ebben a közegben elképzelhetetlen volna az egyén vagy akár a gazdasági szereplők feletti felügyelet még közel hasonló szintjének a kialakítása is, mint amit Kínában láthattunk.*

[96] A nyugati államok okosváros-projektjeiről, azok elvi alapjairól lásd bővebben Szalai Ádám: Az okosváros-koncepciók kritikai földrajzi vizsgálata – elméleti háttér és lehetséges kutatási irányok. *Tér és Társadalom*, 2020/2. szám, 88–107. o.; Rab Judit – Szemerey Samu: *Az okos város fejlesztési modell módszertani alapjai.* Budapest, Lechner Nonprofit Kft., 2018.

[97] Ezzel kapcsolatos jogi dilemmákat lásd bővebben Somkutas Péter – Kőhidi Ákos: Az önvezető autó szoftvere magas szintű szellemi alkotás vagy kifinomult károkozó? *Media Res,* 2017/2. szám, 232–269. o.; Csitei Béla: Az önvezető járművek és az Európai Unió joga. In Lévayné Fazekas Judit – Kecskés Gábor (szerk.): *Az autonóm járművek és intelligens rendszerek jogi vonatkozásai.* Győr, Universitas–Győr Nonprofit Kft, 2020, 55–73. o.

[98] Keserű Barna Arnold: A mesterséges intelligencia néhány magánjogi aspektusáról. In Glavanits Judit (szerk.): *A gazdasági jogalkotás aktuális kérdései.* Budapest, Dialóg Campus, 2019, 109–123. o.

[99] Szigeti Péter: Kapitalizmus és a tőkés termelési mód elmélete. *Eszmélet*, 2019, 1–59. o.; Pongrácz Alex: Az állam gazdaságpolitikai szerepvállalásának változásai. *Pro Publico Bono,* 2017/3. szám, 168–195. o.

[100] Például GDPR rendelet szabályanyaga és gyakorlata. Lásd bővebben Sepsi Tibor: *GDPR útikalauz adatkezelőknek.* Budapest, Wolters Kluwer, 2019. Egyéb területeken is akut problémák forrása: G. Karácsony Gergely: A videójátékok adatkezelési gyakorlata: kommunikáció és profilalkotás. In G. Karácsony Gergely (szerk.): *A videojátékok jogi kérdései.* Győr, Széchenyi István Egyetem, 2021, 25–38. o.

[101] Lásd a svéd és brit példát: Catalin Cimpanu: Sweden and UK's surveillance programs on trial at the European Court of Human Rights. *ZDNet*, 2019. 07. 12.

A kontrolleszközökön túl, a kibertérhez való hozzáférés korlátozása sem képzelhető el olyan mértékben, mivel egyes államok egyenesen alapjogokként tekintenek az internethez való hozzáférésre, de más államok esetében is garanciák garmadája védi azt.[102] Nem beszélve arról, hogy ez jelentősen szembemenne a gazdasági szereplők profitorientált érdekeivel is. Ezek a megállapítások a békeidős, normál működésre igazak, ezeket jelentősen transzformálná egy klasszikus államközi konfliktus, vagy belső rendet támadó szélsőséges események, amelyeket egy teljesen más felhatalmazási közegben kellene az államnak megoldania. Egy ilyen helyzet elkerülése azonban minden érdekelt számára elsődleges érdekké kezd válni.

Az elmúlt évek konfliktusai, társadalmi feszültségei világossá tették, hogy valamiféle elmozdulás szükséges a biztonság digitális terrénumának fokozása frontján is, hiszen lassan a hétköznapok részévé válnak a zsarolóvírusok, a szolgáltatást megtagadó támadások, trollok tevékenysége,[103] amelyek más államokhoz vagy sok esetben a szervezett bűnözéshez kapcsolódtak.[104] A Covid19 járvány mellett megjelent infodémia,[105] vagy a social media platformok szűrőbuborék-gyakorlata,[106] a fake news, a deepfake tartalmak már olyan irányba vitték el a véleménynyilvánítás szabadságát, ahol az egyén már sokszor nem tud különbséget tenni valós és valótlan tartalmak között. Az átlagos felhasználót jelentősen befolyásolják a véleménye, döntése kialakítása során. Az ezekkel szembeni – jogállai keretek közötti – fellépés fontosságát mutatja, hogy az Európai Unió is szorosabb jogi keretek közé kívánja helyezni a közösségimédia-platformok működését, és átláthatóbbá kívánja tenni a szűrési mechanizmusokat is.

Ezek a feszültségek pedig egyértelműen kéz a kézben járnak a hagyományos tér biztonságának korróziójával is, mivel főként a külső szereplő általi szcenáriók abba az irányba is hatnak, hogy negatívan befolyásolják a közbizalmat. Ezeknek a kampányoknak a hatását erősítik, illetve létrejöttét lehetővé teszik egyik oldalról a lawfare,

[102] Gosztonyi, Gergely: The European Court of Human Rights: Internet access as a means of receiving and imparting information and ideas. *International Comparative Jurisprudence Research Journal,* 2020/2. szám, 134–140. o.

[103] Jessika Aro: *Putyin trolljai – Igaz történetek az orosz infoháború frontvonalából.* Budapest, Corvina, 2021.

[104] Mezei Kitti: A szervezett bűnözés az interneten. In Mezei Kitti (szerk.): *A bűnügyi tudományok és az informatika.* Pécs, Budapest, Pécsi Tudományegyetem, MTA TK, 2019, 125–147. o.

[105] A fogalmat a WHO vezette be, és a következőképpen határozta meg: „az infodémia egy problémával kapcsolatos túlzott információáradat, amely megnehezíti a megoldás azonosítását. Magában foglalja az egészségügyi szükséghelyzet során terjedő félretájékoztatást, dezinformációt és pletykákat. Az infodémia hátráltathatja a hatékony népegészségügyi válaszintézkedéseket, továbbá zavart és bizonytalanságot kelthet az emberek körében." Lásd: WHO: Coronavirus disease 2019 (COVID–19) Situation Report – 45. o.

[106] Koltay András: A social media platformok jogi státusa a szólásszabadság nézőpontjából. *In Media Res,* 2019/1. szám, 1–56. o.

vagyis a joggal való rosszindulatú visszaélés[107], valamint az államok jogi sérülékenysége[108] is, amelynek köszönhetően „kételyt, bizalmatlanságot szítsanak és megosszák a társadalmat".[109] Vagyis a transzatlanti térség jogállamisági garanciáit szükségszerűen figyelembe vevő nemzetbiztonsági szabályrendszere ismét a figyelem középpontjába került, ugyanis „ha a védelmi és biztonsági funkciók szabályozása nem kellően korszerű, nem kellően konzisztens, nem kellően stabil és kiszámítható, akkor az az állammal szembeni bizalom erózióját eredményezheti"[110]. Ezzel az általános mechanizmust és az ahhoz kapcsolódó jogrendet is megkérdőjelezik. Így eljutnánk abba a helyzetbe, amit a fejezet felvezetőjében Szigeti Pétert idézve megfogalmaztam, hogy az állami szervek elveszítik társadalmi támogatottságukat, és az egyes szereplők végső soron saját kézbe kívánnák venni a biztonságuk szavatolását, amely anarchiához vezetne, de legalábbis jelentős társadalmi törést hozna létre azok között, akik meg tudják fizetni a saját biztonságukat, és azok között, akik nem. Ami elvezethet ahhoz, hogy a ma ismert alapjai tűnnének el vagy alakulnának át rendszerszinten a transzatlanti térséghez tartozó államoknak.

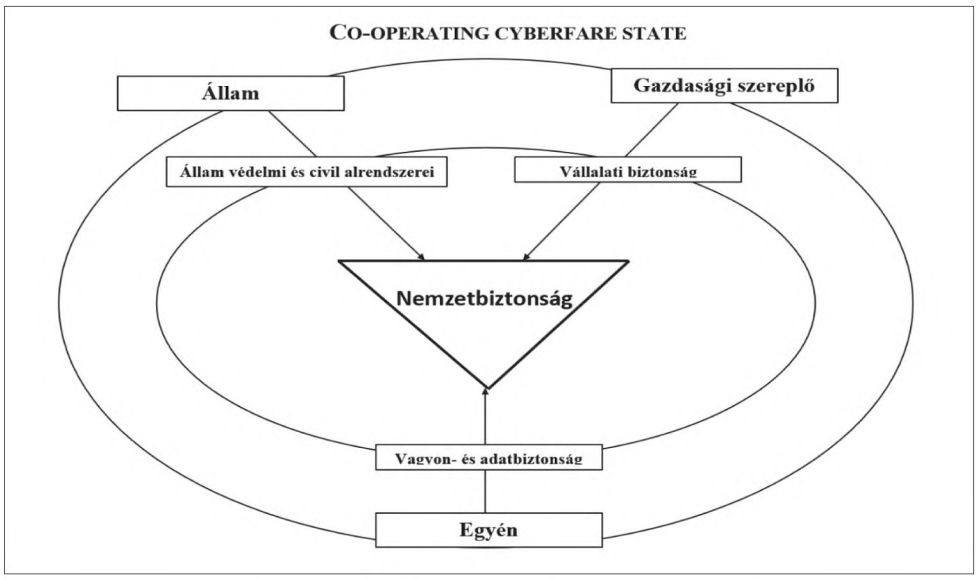
Ezzel pedig meg is érkeztünk ahhoz az indokhoz, amiért a nyugati pólus államainak három fontos szereplője az állam, a gazdasági aktorok és az egyén az együttműködés terepére kell, hogy lépjenek. A cyberfare state a transzatlanti térségben úgy formálható, alakítható ki tehát, hogy közben mindenféleképpen szavatolni kell a jogállam alapvető szegmenseit, de mindeközben meg kell teremteni a biztonsággal való egyensúlyt. Vagyis szemben a smart total control cyberfare state-tel, a totális biztonság felé való elmozdulás nem eredményezheti a szabadság felolvadását. Emellett azonban egyensúlyba kell hozni az egyéni és gazdasági érdekeket a valós biztonsági környezettel. Ugyanis a gazdasági szféra érdekei is a működőképes állami, gazdasági és társadalmi alrendszerek,

[107] A lawfare egy régóta ismert, napjainkban folyamatosan szélesedő, de a hadviselési felfogásból kinövő értelmezési keret, amely a jogi normákat, vagy azok lehetséges értelmezését fordítja a szemben álló fél ellen. Lásd Petruska Ferenc – Vikman László: Egy formabontó hírszerzési nyilatkozat a jogi sérülékenységek szempontjából. *Military and Intelligence CyberSecurity Research Paper,* 2021/4. szám, 1–18. o.; Hódos László: A hibrid konfliktusok felívelési szakasza, avagy a fenyegetés észlelésének, megelőzésének és kezelésének nemzetbiztonsági aspektusai. *Honvédségi Szemle,* 2020/4. szám, 49–64. o.; Farkas Ádám – Resperger István: Az úgynevezett „hibrid hadviselés" kihívásainak kezelése és a nemzetközi jog mai korlátai. In Farkas Ádám – Végh Károly (szerk.): *Új típusú hadviselés a 21. század második évtizedében és azon túl. Intézményi és jogi kihívások.* Budapest, Zrínyi Kiadó, 2020, 132–149. o.; Vikman László: A műveletszervezés jogi feladatai. *Honvédségi Szemle,* 2021/2. szám, 44–56. o.

[108] Szemben a lawfare esetkörével, a jogi sérülékenység a komplex biztonsági felfogáshoz illeszkedő kategória, amely a társadalmi rezíliencia egyik fontos összetevője. Lásd Aurel Sari: Legal Resilience in an Era of Grey Zone Conflicts and Hybrid Threats. *Exeter Centre for International Law Working Paper* 2019/1. szám; Farkas Ádám: *A védelem és biztonság-szavatolás szabályozásának alapkérdései Magyarországon.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2022.

[109] Yvonne Hofstetter: *Láthatatlan háború, avagy miképpen fenyegeti a digitalizáció a világ biztonságát és stabilitását.* Budapest, Corvina, 2020, 85. o.

[110] Farkas Ádám: A kortárs technológia-fejlődés és innováció viszonya a honvédelmi szabályozással. *MTA Law Working Paper,* 2021/4. szám, 4. o.



Co-operating cyberfare state modellje (saját szerkesztés)

amelyek nélkül elképzelhetetlen volna a kapitalista gazdálkodás megfelelő működése, a befektetések biztonságának a szavatolása. Ezt jól mutatják az ukrán–orosz háború jelenlegi gazdasági hatásai és visszásságai, továbbá a már jelzett hosszú távú hatások és törekvések (például Európa energetikai és védelmi önállósítása, mezőgazdasági hatásai stb.), de ezt erősítették a Covid19 világjárvány gazdasági hatásai is, illetve jelentősebb terrortámadásokat követő tőzsdei reakciók is. Az egyén szempontjából az adatai integritása, a tulajdon védelme, a normális életmechanizmusok biztosítása csak működő állami intézményrendszer mellett képzelhető el. Az elmúlt években átalakult biztonsági környezet már alapjaiban támadja ezeket az alrendszereket, aminek rendkívül veszélyes fordulópontját jelenti az orosz–ukrán háború.

Az állam-gazdaság-társadalom kölcsönhatásos fungálására előnyként építő almodellt együttműködő vagy co-operating cyberfare state*-nek nevezhetjük, ahol az együttműködés kiindulópontja szintén a jóléti, szociális digitalizáció. Ennek során a felek között olyan multidiszciplináris megközelítésen nyugvó legjobb gyakorlatot kell kialakítani, amely a jogállami garanciák mellett a biztonság hatékonyságát is előtérbe helyezi. Ennek a legjobb gyakorlatnak magában kell foglalnia az állami szereplők, ezen belül a civil és katonai karakterű szervek*[111] *tapasztalásait, elvárásait, elméleti megközelítéseit, továbbá a gazdasági szereplők ugyanezen aspektusait, valamint a kutatói, innovációs oldalról nem kizárólag a műszaki tudományok képviselőit, hanem a*

[111] Katonai karakterű szervek fogalmáról lásd bővebben Farkas Ádám: A katonai büntetőjog és igazságszolgáltatás helye, szerepe, létjogosultsága az állam és társadalom rendszereiben. *Hadtudomány*, 2012/elektronikus szám, 3–6. o.

társadalomtudományok (jogász, szociológus, közgazdász) és a hadtudomány művelőit is be kell vonni a munkába.[112]

Deklarációk, policyk, stratégia alkotás vonalán számos ilyen együttműködés megvalósulását vetítették előre, amelyek közül több már a megvalósítás pályájára is lépett. Ilyennek tekinthető az egyes kiberbiztonsági stratégiák,[113] a NATO rezilienciaprogramjai,[114] egyes államok kibervédelmi képességeinek kialakítása.[115] Az olyan össztársadalmi problémákat orvosló programok azonban, mint amilyen például az Európai Unió többször meghirdetett, dezinformációval szembeni médiatudatos nevelése, több év elteltével is csak a deklarációk szintjén létezik.[116] E területen érdemi elmozdulást jelenthet az új digitális szolgáltatókkal kapcsolatos jogalkotás,[117] illetve az állami hozzáállás változása.[118] Az egyén szintjéig ható, ténylegesen megvalósuló programokkal azonban nem igazán találkozhatunk, talán azért, mert eddig igazán akuttá a probléma nem alakult, káros hatásai viszont jelentős számban most is megfigyelhetőek.[119]

[112] Farkas Ádám: A multidiszciplinaritás helye, szerepe a védelem és biztonság szabályozásának és szervezésének komplex kutatásaiban. *Közjogi Szemle,* 2021/4. szám, 22–28. o.; Farkas Ádám: A történelmi tapasztalat és a tudomány helye, szerepe a 21. századi védelmi és biztonsági gondolkodásban. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* 2022/1. szám.

[113] Vikman László: Gondolatok a kiberbiztonsági stratégiák fejlesztésére vonatkozó nemzetközi útmutató kapcsán. *SmartLaw Research Group Workin Paper*, 2022/1. szám.

[114] Lásd Molnár Ferenc: A reziliencia kérdése és a NATO. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok*, 2021/15. szám; Farkas Ádám – Spitzer Jenő: Az információs korszak és az állami reziliencia egyes kérdései. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok*, 2021/18. szám; Keszely László: Hibrid hadviselés és nemzeti ellenálló képesség (resilience), avagy átfogó megközelítés újratöltve. *Katonai Jogi és Hadijogi Szemle*, 2018/1. szám, 29–62. o.; Vikman László: A közműszolgáltatások és a reziliencia egyes kérdései, különös tekintettel a kiberbiztonságra. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok*, 2021/14. szám.

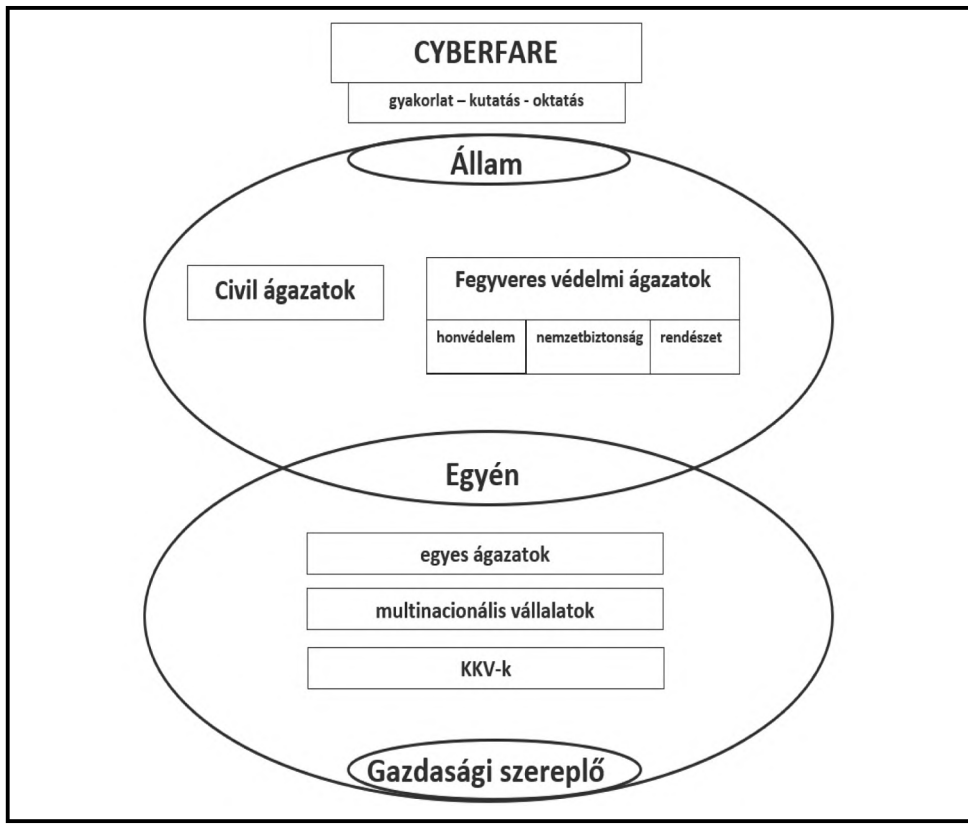
[115] Farkas Ádám: Kibertér művelet: hírszerző, rendészeti és katonai műveletek elegye? Gondolatok az angol National Cyber Force kapcsán. *Military and Intelligence CyberSecurity Research Paper*, 2021/1. szám; Vikman László: A német kiberbiztonsági szisztéma áttekintése: Szervezeti keretek, különös tekintettel a nemzetbiztonsági szolgálatok és a hadsereg szerepére és kapcsolatára, valamint a szabályozási háttér alakulására. *Military and Intelligence CyberSecurity Research Paper*, 2021/2. szám.

[116] Az Európai Bizottság és az Unió Külügyi és Biztonságpolitikai Főképviselőjének közös közleménye – Cselekvési terv a félretájékoztatással szemben, Brüsszel, 2018. 12. 15., Join(2018)36. Final; Az Európai Bizottságnak közleménye az Európai Demokráciára vonatkozó cselekvési tervről. Brüsszel, 2020. 12. 3. COM(2020) 790 Final.

[117] Az Európai Bizottság javaslat Az Európai Parlament és a Tanács rendelete a digitális szolgáltatások egységes piacáról (digitális szolgáltatásokról szóló jogszabály) és a 2000/31/EK irányelv módosításáról, Brüsszel, 2020. 12. 15., 2020/0361(COD).

[118] Gosztonyi Gergely: Az internetes tartalomszabályozással kapcsolatos új gondolkodási irányok az Amerikai Egyesült Államokban. *Miskolci Jogi Szemle*, 2021/4. szám, 40–54. o.

[119] Mary Aiken: *Cyber-csapda – Hogyan változtatja meg az online tér az emberi viselkedést?* Budapest, Harmat – Új Ember, 2020; Douglas Murray: *A tömegek tébolya – Áldozatok a politikai korrektség oltárán?* Budapest, Alexandra, 2020.



Az egyén relevanciája kibertérben a co-operation cyberfare state esetében
(saját szerkesztés)

A jogállami keretek között működő cyberfare state esetében, a 21. század biztonsági környezetében nem hagyható figyelmen kívül az egyén szerepe sem; nem véletlen, hogy a konkuráló államok mindent megtesznek annak érdekében, hogy az egyént, az egyéni döntés szabadságát kikapcsolják, hiszen a rendszer szempontjából a legjelentősebb biztonsági kockázatot továbbra is az emberek, az egyének jelentik. Ebből adódóan a co-operating almodell államainak jogállami keretek közötti válaszokat kell találniuk erre a kérdésre is, jelenleg azonban az látszik, hogy nem igazán tudnak mit kezdeni az egyéni szereplők tömegével, nem igazán tudják a helyüket definiálni a biztonsági környezetben, annak ellenére – ahogy a lenti ábrán látszik is –, hogy mind az állam, mind pedig a gazdasági szereplők alrendszereiben aktívan közreműködnek.

Az egyének munkaerőként és fogyasztóként is aktív szereplők, akik mindkét szerepükben potenciális veszélyforrások az állami és gazdasági rendszerekre, és természetesen ugyanekkora mértékben a saját adatvagyonukra vagy hagyományos tulajdonukra. Így szükségszerű volna meghaladni azt a felfogást, hogy az egyéni

felelősség szintjére engedjük ezeknek a problémáknak a megoldását, amelyben még magára is hagyjuk az egyes szereplőket, azoknak tényleges tudásától, képzettségi szintjétől függetlenül. E körben az együttműködés állami vonatkozásai és különösen a védelmi-biztonsági szegmense kapcsán is komoly lemaradást kell ma behozni a biztonságtudatosság szintjén, amivel a kibertérrel összefüggő biztonságfelfogást is szinkronizálni kell.[120]

Ezen államok esetében átfogó oktatási projekteket kell kidolgozni az iskolarendszer minden szintjén, hiszen ma már nemcsak kizárólag a magas kvalifikációt megkövetelő munkakörökben kerülnek az emberek kapcsolatba a kibertérrel és annak egyes alrendszereivel, hanem azok a hétköznapok részévé is váltak.[121] Fájdalmasan kijózanító jelenségként lehetett elkönyvelni, hogy az okoseszközök világában, például a Covid19 ellen védő vakcinákra történő regisztrációs rendszer elérése, kitöltése egyes egyének számára megoldhatatlan feladatot jelentett (itt nem a rendszer eléréséhez szükséges infrastruktúra hiányára kell gondolni, vagy az idős állampolgárokra), míg ugyanők a hétköznapok során számos rendszerhez férnek hozzá. Ma már a felsőoktatásban sincs olyan oktatási terület, amelynek képzésébe ne volna feltétlenül szükséges beépíteni ezeket a készségeket, mert adott esetben vezetőként fog ezek hiányában dönteni az egyén a területet is érintő fontos kérdésekről, vagy ezeket nem ismerve működtet társadalmi alrendszert a potenciális veszélyforrásokat fel nem ismerve, ismertetve (például óvodai, iskolai nevelés). S legalább ugyanilyen fontos ezekben a problémákban a nyomon követés kérdése, hiszen a mindenkori új kihívásokhoz kell igazítani magát a képzést is. Ezek megvalósítása tovább már

[120] Bányász Péter – Krasznay Csaba – Tóth András: A NATO kibervédelmi szakpolitikája. Szenes Zoltán (szerk.) *A mai NATO: A szövetség helyzete és feladatai.* Budapest, HM Zrínyi Térképészeti és Kommunikációs Szolgáltató Nonprofit Kft., 2021, 130–149. o.; Annamária Beláz – Csaba Krasznay – Zsolt Szabó: Cybersecurity Strategy and Leadership Managment Issues. In Živan Živković (szerk.): *An international serial publication for theory and practice of Management Science – IMCSM Proceedings(2020)*, Bor, University of Belgrade, Technical Faculty in Bor, Engineering Management Department (EMD), 2020, 242–252. o.; Kiss Attila – Krasznay Csaba: A felhasználói viselkedéselemzés kiberbiztonsági előnyei és adatvédelmi kihívásai. *Információs Társadalom: Társadalomtudományi Folyóirat*, 2017/1. szám, 55–71. o.; Farkas Ádám: A védelmi-biztonsági gondolkodás és képzés megújításának elméleti és kulturális alapjai. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok*, 2022/2. szám.

[121] A sérülékenységet és az oktatás szükségességét jól példázza az alábbi megállapítás: „Minden IT-biztonsági szakértő tisztában van vele, hogy a kibertérben a leggyengébb láncszem a humán faktor; a munkavállalók, akik – emberi természetükből fakadóan – jóhiszeműek, megtéveszthetőek, megfélemlíthetőek, nincsenek is tisztában a lehetséges kockázatokkal; éppen azért az ún. social engineering támadások célpontjai. Napjaink digitalizált világában minden munkavállaló kapcsolatba kerül számítógépes rendszerekkel, bizalmas adatokat kezel, és éppen ezért potenciális rizikóforrás. Ez a kockázat tovább növekszik azáltal, ha a munkavállaló a céges környezeten kívül, mérsékelt ellenőrzés mellett tevékenykedik." Németh Richárd: A COVID-19 járvány okán bevezetett Home Office munkavégzés hatása a munkakörülményekre és szervezeti kommunikációra nagyvállalati környezetben. *Jog Állam Politika*, 2021/4. szám, 101. o.

nem várathat magára,[122] hiszen a káros hatások már ténylegesen megindítottak akár deviáns folyamatokat is a társadalmon belül,[123] amelyek a halogatás révén nehezen visszafordíthatóak. Nem feledve az alapfelvetést, ha ezeket a társadalmi, biztonsági kihívásokat nem tudják kezelni a transzatlanti régió államai, abból végső soron az ellenpólus államainak intézményes győzelme is kialakulhat, amellyel önnön képét veszítheti el a régió.

****

A cyberfare state mindegyik modelljében a kiindulópont a kibertérhez kapcsolódó rendszerek által az állam jóléti, szociális rendszereinek reformja, valamint a szolgáltató közigazgatás újradefiniálása. Emellett viszont jelentős eltérések mutatkoznak abban, hogy miként viszonyulnak ezeknek a rendszereknek a védelem és biztonságszavatolás (angolszász megközelítésben: nemzetbiztonság) területén történő alkalmazásához.

A smart total control cyberfare state államfelfogása e körben visszanyúl a warfare state egyes jegyeihez, fúziót képez a gazdasági szereplők és az állam között, amelynek eredményeként a lehető legteljesebb mértékben kívánja kontrollálni polgárait és a kiberterét. Ennek során kidomborítják az állam hatalmi aspektusait, és saját biztonságuk szavatolását csak a hatalom révén, az erő által látják biztosítottnak. Így a „külső" kibertérben is aktívan használják a modern technológia által biztosított eszközöket.

A nyugati államok esetében is jelentős mértékű volt a digitalizáció, így eme folyamatok jelentős hatást gyakoroltak a társadalomra, gazdaságra, és beágyazódtak a közigazgatási alrendszerekbe is. Az államra gyakorolt hatásuknak köszönhetően megteremtették a co-operating cyberfare state alapjait, vagyis a szereplők közötti folyamatos interakciót. Azonban a pozitív hozadékok mellett, mint fentebb láttuk, számos negatív biztonsági tapasztalás is hatással volt ezen típusú államokra is, így az állami és nem állami szereplők által képviselt erőszakos, jogellenes fenyegető fellépések és támadások kibereszközökkel való felerősítése, illetve a hagyományos fenyegetések kibertéri lehetőségekkel való kombinálása. Amely szükségszerűvé teszi, hogy ezen államok esetében fokozódjon az egyes szereplők közötti együttműködés. Ebben viszont jelentős eltérés mutatkozik a másik almodellhez képest, hiszen az egyénhez való viszonyulás teljesen más képet mutat, mert a jogállami keretek (béke-idős) megtartása nem teszi lehetővé a polgárok fenti mértékű korlátozását. Sajátos,

[122] Erre is tökéletes példa az infodémia kérdésköre, amikor az emberek jelentős hányada hitt el olyan fake news híreket, amely szerint az oltások HIV-et okoznak, chipet ültetnek az emberi szervezetbe, népirtást követnek el velük, stb. (https://www.webbeteg.hu/cikkek/fertozo_betegseg/17762/tenyek-es-tevhitek-az-oltasokrol).

[123] Kiss Tibor: *Agresszió a cybertérben.* Budapest, Nemzeti Közszolgálati Egyetem, 2020; Kiss Tibor – Pari Katalin – Prazsák Gergő: *Cyberdeviancia.* Budapest, Dialóg Campus, 2019.

hogy szemben a másik almodellel, ebben az almodellben az egyes szereplők alapvetően ellenérdekeltek, mégis a megváltozott környezetben szükségszerű az együttműködésük. Ezen kooperációnak a biztonsággal kapcsolatos területek valamenynyi szegmensére ki kell terjednie, kiemelten a modern technológia vívmányaira. Az együttműködésnek pedig egy legjobb gyakorlatot kell létrehozni, megújítva a jelenlegi alrendszereket.

A kialakított rendszernek nem eseti jelleggel, nem pillanatnyi kihívásokat kell kezelnie, hanem átfogó, rendszerszintű és hosszú távú megoldást kell létrehoznia, mindezt a jogállami attribútumok fenntartása mellett. „Rendeltetése ugyanis a totálissá váló biztonsági kihívások megelőzésén, elhárításán, illetve felszámolásán túl pontosan az, hogy kitörjünk a my lai-i, abu ghraibi, guantanamoi és egyéb árnyékokból, s valóban rendezett, átgondolt, a kor kihívásaihoz igazodó, de egyben jogállami"[124] *biztonsági modellt, legjobb gyakorlatot teremtsünk meg.*

Azt is látni kell, hogy univerzális, minden államra, régióra alkalmazható megoldások nincsenek. A transzatlanti térség államai kulturálisan és történeti hagyományaikat tekintve rendkívül sokszínűek, így a kialakítandó rendszer esetében a nemzeti sajátosságokat, történeti, társadalmi tradíciókat szükséges figyelembe venni. Emellett az egyes megoldásoknak idomulniuk kell az alkalmazott szinthez, hiszen más igény formálódik meg egy multinacionális vállalatnál és egy KKV esetében, illetve egy helyi önkormányzat vagy országos szerv esetében. Az ellenőrzés, visszacsatolás, elemzés szükségszerű velejárója a rendszernek. A co-operating cyberfare state legjelentősebb kihívása az egyén elhelyezése ebben a rendszerben, tudatosságának kialakítása, megerősítése alapvető fontosságú a rendszer fenntartása, védelme és működtetése érdekében, amelyben a képzés, oktatás kiemelten hangsúlyos szerephez jut.

Ezen co-operating cyberfare state rendszereinek kialakítása átfogó reformot igényel, ami nélkül az átalakult biztonsági környezet kihívásaival (például hibrid konfliktusok ezen belül is kibertámadások, dezinformációk, radikalizmus, [kiber]terrorizmus stb.) hosszú távon nem tudnak eredményesen megküzdeni a transzatlanti térség államai. *A reformnak pedig ténylegesnek és átfogónak kell lennie, és az orosz–ukrán háború geopolitikai történéseit látva azonnal meg kell indítani, ahol – az elmúlt évtizedek tapasztalásaival szemben – a reform nem abban rejlik, hogy a múlt fáradt és kopott ötleteit leporoljuk és újracsomagoljuk. Az igazi reform csak akkor valósulhat meg, ha elfogadjuk az új paradigmát, és újradefiniáljuk az állam szerepét.*[125]

[124] Farkas Ádám: *A totálitás kora? A 21. század biztonsági környezetének és kihívásainak totalitása és a totális védelem gondolatkísérlete.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2018, 70. o.

[125] Gregory M. Kaladijan: Welfare vs Cyberfare. *Journal of Children and Proverty*, 1996/1. szám 103. o.

PONGRÁCZ ALEX

Gondolatok a kibertér és a digitalizáció állammodellkérdésre gyakorolt hatásairól

Az államok rendszerezésének kérdése – az állammal kapcsolatos egyéb „rejtélyekhez" hasonlóan – régtől fogva foglalkoztatja a gondolkodók fantáziáját. Erre figyelemmel egyáltalán nem meglepő, hogy az évszázadok folyamán számos-számtalan szempontból tették vizsgálat tárgyává az államot az államelmélet ismert és/vagy elismert művelői – mondhatni, hogy e kitüntetett érdeklődésnek köszönhetően nagyfokú „típus-pluralizmus" érvényesül.[1] Georg Jellinek szerint az államtan története „nem kis részben az arra irányuló kísérletek története, hogy fölismerjék a tipikus államot"[2] – így aztán (elsősorban a modern állam történelmi és koncepcionális típusai szerinti osztályozás,[3] illetőleg az állami mozgáspálya egyes csomópontjai[4] mentén) az államot annak elemzői számtalan jelzővel látták el.[5] Amennyiben az államszervezet szempontjából szemléljük az egyes politikai közösségek formáit, a szervezett közhatalom típusait illetően szintén különböző jelzőkkel ellátott kategóriákat nevezhetünk meg. Carl Schmitt a szinte permanens jelleggel az összeomlás szélén táncoló ún. weimari Németország belpolitikai helyzetének elemzése során például – az arisztotelészi és montesquieu-i hagyományt ápolva, s azt legfeljebb konkrét elnevezéseiben módosítva – törvényhozó, kormányzó vagy igazgató, valamint igazságszol-

[1] Ennek rövid áttekintésére nézve lásd Péteri Zoltán: Az államok rendszerezése: államtípusok és államformák. In Takács Péter (szerk.): *Államelmélet. Előadások az államelmélet és az állambölcselet köréből.* Miskolc, Bíbor Kiadó, 2001, 94–121. o. (A típus-pluralizmus szófordulata e munka 112. oldalán található.)

[2] Georg Jellinek: *Általános államtan.* Budapest, ELTE ÁJK TEMPUS Összehasonlító Jogi Kultúrák, 1994, 45. o.

[3] Takács Péter: *Államtan. A modern állam és elmélete. Két fejezet az állam általános elmélete köréből.* Budapest, Nemzeti Közszolgálati Egyetem, 2012, 133–154. o.

[4] Szigeti Péter: Az állam mozgáspályájának átfogó íve és csomópontjai a jelenkorban. In Egresi Katalin et al.: *Államelmélet.* Győr, Széchenyi István Egyetem Deák Ferenc Állam- és Jogtudományi Kar Jogelméleti Tanszék, 2016, 260–265. o.

[5] Hozzá kell tenni ugyanakkor, hogy amennyiben nem a különböző „jelzős szerkezetek" felől nézve vizsgáljuk az államot, akkor annak rendszerezésére és minősítésére két kategória – ti. az államforma és az államtípus – kitűnően alkalmasnak ígérkezik. Lásd Takács Péter: Észrevételek az államforma fogalmához. *Jog – Állam – Politika.* Ünnepi különszám Kukorelli István tiszteletére. 2022/2. különszám, 365–389. o. Az alábbiakban – az általunk vizsgált téma specifikumaira tekintettel – ezt a fajta osztályozási lehetőséget nem vizsgáljuk kiterjedtebben.

gáltató államtípusok között tett különbséget.[6] A nyugat-európai szakirodalomban első ízben William Temple canterburyi érsek által használt,[7] a hatalmi államtól való világos distinkció igényét kifejezésre juttató jóléti állam *(welfare state)* típusa pedig a második világháborút követően hosszú évtizedekig gyakorolt befolyást a nyugat-európai társadalmak működésére, reprezentálva a demokratikus berendezkedéssel bíró államok kormányzatainak jólét iránti elkötelezettségét.

Az állam imént említett különböző típusai általában a hatalommegosztás vagy a közjóléti és gazdasági funkciók fókuszpontja felől közelítik meg a szervezett közhatalom működését. Hasonló logika mentén gondolkodva, ugyanakkor a fenti, klasszikussá nemesedett tipizálásokat – és a szerintünk alapvetően állam- és alkotmánytörténeti karakterű állammodell terminusát[8] – újragondolva beszélhetünk a digitalizáció folytán (is) folyamatos kihívásoknak és kockázatoknak kitett államra vonatkoztatva az ún. *cyberfare state* fogalmáról, vagy Kelemen Roland terminológiájával élve: állammodelljéről.[9] A digitalizáció robbanásszerű fejlődése és terjedése ugyanis jelentős hatást gyakorolt az államok és társadalmak szerkezetére, szabályozására, politikai és biztonsági vonatkozásaira egyaránt. Ebből is következik, hogy nem Kelemen az egyetlen szerző azonban, aki a digitalizációval összefüggésben új állammodell vagy kormányzási modell kialakulásáról beszél: ti. Varga Csaba és Ugrin Emese már 2007-ben azt állították, hogy a részvételi állam (más megjelölésekkel: közvetlen állam, digitális állam, tudásközpontú állam, sőt magas rangú köztu-

[6] Carl Schmitt: *Legalitás és legitimitás.* Máriabesnyő–Gödöllő, Attraktor Kft., 2006, 7–21. o.

Hozzá kell ugyanakkor tenni, hogy ezek az államtípusok csakis elméleti célok szolgálatába állított, konstruált ideáltípusok, amelyek tiszta formában nem valósulhatnak meg. Ennek bővebb elemzésére nézve lásd Cs. Kiss Lajos: A totális állam elmélete és mítosza. *Világosság*, 2010/51. szám (ősz), 19–63. o.

Ugyancsak az „elvont okoskodásokból" folyó tipizálások időnként hiábavaló mivoltára hívta fel a figyelmet Ferdinandy László, akinek nehezen vitatható meglátása szerint „az állam a valóságban helyenkint és koronkint… különböző és folyton változó formában jelentkezik a szerint, hogy a társadalom korszerű és egyéb speciális szükséglete és a történelmi fejlődés mint hozza magával". Ferdinandy László: Államalakulatok és államalkotó eszmék. Történelembölcseleti tanulmányok III. *Magyar Kultura [Kultúra]*, 1924/10. szám, 529. o.

[7] William Temple: *Citizen and Churchman.* London, Eyre & Spottiswoode Publishers, 1941, 35. o.

[8] A Mezey–Gosztonyi szerkesztőpáros által jegyzett magyar alkotmánytörténeti tankönyvben például Mezey Barna és Képes György a patrimoniális, a rendi, az abszolút monarchia, valamint a polgári állam állammodelljeiről beszélnek. Lásd Mezey Barna – Gosztonyi Gergely (szerk.): *Magyar alkotmánytörténet.* Budapest, Osiris Kiadó, 2020, 77–114, 293–355. o. Emellett – a demokratikus állammodellektől megkülönböztetendő – önálló kategóriát képeznek az ún. diktatórikus állammodellek is.

[9] Kelemen Roland: Cyberfare state – Egy hibrid állammodell 21. századi születése. *Military and Intelligence CyberSecurity Research Paper,* 2022/1. szám. Az egyén cyberfare state modelljében elfoglalt helyének vizsgálatára nézve lásd Kelemen Roland – Mihály Laura Dominika: A kibertér és a psziché ütközéspontjai mint a 21. századi reziliencia kulcskérdése. *Védelmi-biztonsági Szabályozási és Kormányzástani Kutatóműhely*, 2022/14. szám. A kibertér társadalmi hálózatokra gyakorolt hatásaira nézve pedig lásd Kelemen Roland – Németh Richárd: Társadalmi hálózatok és reziliencia. *Védelmi-Biztonsági Szabályozási és Kormányzástani Kutatóműhely*, 2022/13. szám.

dat által vezetett állam) állammodellként egy alapvető paradigmaváltást feltételez. „A részvételi állam… alapvetően nem politikai hatalmi állam, hanem egyszerre közösségi és személyes állam, amely minden olyan erőforrást (közvetlen demokrácia, globális innovációs és tudásközpontú kor stb.) mozgósítani akar, amely a régi és új univerzális és lokális problémák kezelésében alkalmazható."[10]

Kelemen egyébként a Gregory M. Kaladjian *Welfare vs. Cyberfare* című tanulmányában[11] szereplő megállapításokból indul ki, amelyben az amerikai szerző a jóléti állam gyakran hangoztatott reformjának szükségességét vázolta fel, különös figyelmet fordítva az elektronikus rendszerek szociális igazgatásba történő adaptálására. Kaladjian szerint a kibertérben rejlő lehetőségek kiaknázása hatékonyabbá teheti az állami funkciókat – a szociális igazgatás működésmódját legalábbis mindenképpen. E gondolat – némi fantáziával – akár a közigazgatás-tudomány elismert poeta doctusától, Magyary Zoltántól is származhatna, aki már a két világháború között elismeréssel viseltetett a technológiai újítások (Schmitt szavaival: a technikai haladás örvényébe kerülés[12]) iránt, s a közigazgatás modernizációját, valamint a haladásért folytatott küzdelmet[13] – tehát az állampolgárok boldogításáért és a nemzetközi „kemény versenyben" lehetőleg nagy hatásfokkal való részvételt[14] – minden állam számára kötelességként tételezte. Kaladjian a tanulmány megjelenésekor, 1996-ban nem kevesebbet állított, mint hogy „A jelenlegi és korábbi [szak]politikák és a meglévő kulturális szokások felülvizsgálatával a jóléti rendszer újjáteremthető, és egy új paradigmára támaszkodhat: a cyberfare-re… Bár a cyberfare inkorporálása és a jóléti rendszer reformja nem mentes a kihívásoktól, az amerikai társadalom szegénységi problémájának megoldása szempontjából [mégis] létfontosságú."[15] Kaladjian – akárcsak egykoron Magyary – az igazi „információs boom" bekövetkezte előtt talán magányos prófétának bizonyult, ám napjainkra már az államigazgatás egésze képviselteti magát a kibertérben. (Érdekességként említhetjük meg, hogy a görög eredetű *κυβέρνησις [kübernézisz]* a szabályozás vagy kormányzás jelentéstartalma értelmében a kormányzati metaforák egyik legrégibb formáját jelenti, s különböző

[10] Ugrin Emese – Varga Csaba: *Új állam- és demokráciaelmélet.* Budapest, Századvég Kiadó, 2007, 69. o.

[11] Gregory M. Kaladjian: Welfare vs. Cyberfare. *Journal of Children and Poverty*, 1996/1. szám, 93–104. o.

[12] Carl Schmitt: A partizán elmélete. In Carl Schmitt: *A politikai fogalma. Válogatott politika- és államelméleti tanulmányok.* Budapest, Osiris – Pallas Stúdió – Attraktor, 2002, 150. o.

[13] Magyary Zoltán: *Küzdelem a haladásért.* Kézirat. 1944. (http://real-ms.mtak.hu/15898/1/Ms_10640_1.pdf).

[14] Magyary Zoltán: Két korszak mesgyéjén [mezsgyéjén]: Jogállam – a cselekvő állam. *Bányászati és Kohászati Lapok* 1939/6. szám, 110. o. Az ún. cselekvő állam átfogó elemzésére nézve lásd például Szabadfalvi József: Jogállam – cselekvő állam: Magyary Zoltán jogállam-felfogásának rekonstrukciója. *Pro Futuro*, 2022/1. szám, 1–15. o., illetve Szűrös Éva et al. (szerk.): *„A cselekvés állama". Dr. Kiss István emlékkötet.* Budapest, Agroinform Kiadó, 2006.

[15] Kaladjian: i. m. (1996), 93. o.

kontextusban gyakran tűnik fel kormányrúdként, az „állam hajójának irányításaként" vagy éppenséggel *manus gubernatoris*ként.)[16]

Így a kibertér sajátos „evolúciója" nemcsak a jóléti állam reformját kényszerítette ki, hanem „egy teljesen átalakult struktúrájú társadalmi-gazdasági közeget [is] eredményezett", ami az állami funkciók teljes spektrumát érintette.[17] Napjainkban a Szuverén – amint azt a mottó gyanánt választott idézet is mutatja – egyes megközelítések szerint egyenesen az, aki a tudományos-technikai eszközök felett a leghatékonyabban képes diszponálni; Schelsky szerint már az ipari társadalmakban is teljesen összeolvadt a szuverenitás ténye a technológiai eszközök alkalmazásával. A modern technikai rendszerek szerinte sui generis megoldásokat generáltak, és saját (műszaki elvek feletti) döntéseket írhatnak elő, a klasszikus értelemben vett szuverenitás pedig felhígul a „szociotechnikai hálózatokban".[18] „A technikailag keresztül-kasul szervezett világ immanens racionalitása" tehát maradéktalanul juthatott érvényre, és „a technikai-funkcionalisztikus folyamatok súrlódásmentesen" mehettek végbe.[19] Ebben a világban a partizán lehet ugyan zavarkeltő – mint egy kutya az autópályán, à la Schmitt[20] –, azonban a trollhadseregek katonái – a hackerekhez hasonlatosan – éppen hogy felértékelődnek, s közel sem közlekedésrendészeti problémát jelentenek.[21] (A szellemi és politikai partizánok pedig ezzel párhuzamosan az állam – s mondjuk ki, a kibertér egyéb notabilitásai – technológiai hatalmát reprezentáló technoszférával szemben az őserdőbe visszavonuló egyéni szabadságharcosokká fokozódnak le.)[22]

A digitalizáció Janus-arcúsága, amely egyszerre hordoz magában pozitívumokat és páratlan lehetőségeket, valamint negatívumokat – mások mellett az informatikai forradalom és a digitális pénzügyi világháló révén tovább mélyülő társadalmi

[16] Nicolas Guilhot: Automatic Leviathan: Cybernetics and politics in Carl Schmitt's postwar writings. *History of the Human Sciences*, 2020/1. szám, 130. o.

[17] Kelemen: i. m. (2022), 2. o. Ennek bővebb elemzésére nézve lásd Farkas Ádám: *Az állam fegyveres védelmének alapvonalai.* Budapest, Katonai Nemzetbiztonsági Szolgálat, 2019, illetve Farkas Ádám: *A védelem és biztonság-szavatolás szabályozásának alapkérdései Magyarországon.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2022; Vikman László: A közműszolgáltatások és a reziliencia egyes kérdései, különös tekintettel a kiberbiztonságra. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok* 2021/14. szám; Petruska Ferenc – Vikman László: Egy formabontó hírszerzési nyilatkozat a jogi sérülékenységek szempontjából. *Military and Intelligence CyberSecurity Research Paper* 2021/4. szám.

[18] Schelsky: i. m. (1961); Guilhot: i. m. (2020), 134. o.

[19] Schmitt: i. m. (2002), 151. o.

[20] Schmitt: i. m. (2002), 151. o.

[21] Ennek bővebb elemzésére nézve lásd Kelemen Roland: A nem állami kibertéri műveletek egyes szereplőinek jelentősége a hibrid konfliktusokban. *Smart Law Research Group Working Paper*, 2021/2. szám.

[22] Ernst Jünger: *Waldgang.* Stuttgart, Klett-Cotta, 1980; Békés Márton: Erdei séta (Waldgang-kommentár). In Békés Márton: *Az utolsó felkelés.* Budapest, Századvég Kiadó, 2014, 60–65. o.; Guilhot: i. m. (2020), 132. o.

egyenlőtlenségeket és a Big Data révén a közösségi gráfok felhasználási lehetőségeinek, valamint az ún. adatbáróknak való nagyfokú kiszolgáltatottságot[23] –, Kelemen tézise szerint egy korábban nem tapasztalt hibrid állammodellt hozott létre *a cyberfare state* égisze alatt.

Kelemen megállapításával, miszerint „a jóléti állam egyes attribútumait erősítő államfelfogás tud csak eredményesen fellépni" a 21. század kihívásaival szemben, e sorok írója maximálisan egyetért. Az alkotmányos úton korlátozott, ugyanakkor a szabadpiac kudarcait megfelelően kezelni és korrigálni képes, a szükséget szenvedő állampolgárai érdekében fellépő, ezért hatékony és erős állam valóban elixírt jelenthet turbulens, gazdasági, pénzügyi, biztonsági és ökológiai krízisektől egyaránt sújtott világunkban. Az, hogy az információs társadalom ideológiája által katalizált digitalizáció e missziós küzdelem csatasorába állítható-e, jelenleg nyitott kérdés, mindenesetre őszintén reméljük, hogy a feltett kérdésre szolgáltatott válasz „igenlő" lehet. A digitalizáció nyomában megvalósulni-kiépülni látszó digitális (hálózati, elektronikus) állam és közigazgatás,[24] valamint az e-közszolgáltatások széles köre valóban számos szegmensében voltak képesek tehermentesíteni a mindennapjainkat, a „söralátét méretű adóbevallást" is felváltó e-szja-rendszertől kezdve egészen az ügyfélkapus rendszer által nyújtott megannyi szolgáltatásig. Ezzel az állam mintegy eleget is tett a neoliberális közmenedzsment-felfogás által rendre csak szajkózott, a neoweberiánus felfogás keretei között azonban központi jelentőségűvé váló polgár- és felhasználóbarát, szolgáltatásorientált közigazgatás ars poeticájának.[25]

Nem hallgathatók el azonban e nagyfokú digitalizáció árnyoldalai sem, s kérdéssel foglalkozó szerzők e hátrányok lajstromba vétele elől sem futamodhatnak meg. A szolgáltatásközpontúság és az adatokhoz való hozzáférés lehetősége ugyanis „a klasszikus *welfare state* egyenlőségre törekvő oldalát elmozdította egy elitista működés irányába, ahol [az] ezen erőforrások feletti tényleges rendelkezés lehetősége teremti meg a döntéshozásnak az alapjait. Tökéletes példái ennek a magántulajdonban álló okosvárosok, ahol az adatok szinte teljességéhez hozzáférnek az olyan nagyvállalatok, mint az Amazon Seattle-ben, vagy Facebookville, Zucktown esetében a Meta … . Szintén az adatok garmadája felett diszponálnak a *social media* vállalatok, azokat tényleges termékként kezelik."[26] 1948-ban Dominique Duparle dominikánus szerzetes egy olyan új korszak kontúrjait rajzolta fel, „amelyekben egy irányító masina fogja helyettesíteni … a politikára manapság nyilvánvalóan alkalmatlan fe-

[23] Erre nézve bővebben lásd Forgács Imre: *Az eltűnő munka nyomában. A Big Data és a pénztőke évszázada.* Budapest, Gondolat Kiadó, 2015, különösen 59–85. o.

[24] Ennek mélyebb elemzésére nézve lásd Varga Csaba: Az állam és a közigazgatás új elmélete. *Polgári Szemle*, 2006/2–3. szám.

[25] Ennek bővebb leírására nézve lásd Pongrácz Alex: A közmenedzsment-reformok metamorfózisai. *Új Magyar Közigazgatás*, 2016/1. szám, 1–12. o.

[26] Kelemen: i. m. (2022), 6–7. o.

jeket és a megszokott, de kormányzásra alkalmatlan apparátusokat".[27] Pierre Musso több mint hét évtizeddel később a következőképpen replikázott a páter disztopikus víziójára: „Amit Duparle páter az állam kiber-tengeri kígyójaként képzelt el, manapság olyan óriásvállalatok formájában jelenik meg, mint a Google, az Amazon, a Facebook, az Apple vagy a Microsoft. Ez lenne a Szilikonvölgy politikai projektje."[28] Forgács Imre szerint az „adatok diktatúrája" egyre fenyegetőbbé válik a közösségi oldalakon. Az „adatosítás" révén a történelemben példa nélküli hatalom koncentrálódhat egy-egy magáncég „adatbáróinak" kezében. „Talán a lájkolás leglelkesebb hívei sem tudnak róla, de a Facebooknak már 2012-ben is körülbelül egymilliárd felhasználója volt, s a közöttük meglévő ismeretségek száma még a 100 milliárdot is meghaladta. … A diktatúra veszélye éppen abban rejlik, hogy a társadalmi kapcsolatokat rögzítő ún. közösségi gráf *(social graph)* felhasználási lehetőségei csaknem korlátlanok."[29] Az Amazonhoz, a Google-hoz vagy a Facebookhoz tartozó, élenjáró cégek teljesítménye jelentős részben a vevők és felhasználók interakcióiból megszerzett digitális lábnyomoknak köszönhető, az ezekből levont következtetéseket pedig rendre beépítik a szolgáltatásaikba. A Facebook auditált pénzügyi beszámolója szerint a cég 2012-ben, a tőzsdére történő belépésekor „mindössze" 6,3 milliárd dollárt ért, ami elsősorban a számítógépes hardvert, az irodai berendezéseket és más materiális javak könyv szerinti értékét jelentette. A piac viszont a részvények kibocsátásakor 104 milliárd dollárra értékelte a Facebookot; ennek hátterében az áll, hogy a befektetők az „immateriális javakért", azaz a gigantikus információmennyiségben rejlő üzleti lehetőségekért voltak hajlandók sokszorosan többet fizetni.[30] Miközben a 21. századi technológia „szép új világában" az algoritmusok számára lehetővé teszik, hogy „meghackeljék" az emberiséget,[31] a világhálón jelen lévő nagyvállalatok (az ún. GAFA, azaz a Google, az Amazon, a Facebook és az Apple) olyan mértékű gazdasági befolyást szereztek, amely már a hatalmi játszmákba történő beszállást is lehetővé tette számukra.[32] 2018 tavaszán valóságos bombaként robbant a hír, hogy Donald Trump kampánystábja mintegy 50 millió Facebook-felhasználó adataihoz fért hozzá a Cambridge Analytica (CA) adatbázisának segítségével. Aleskandr Kogan, a cambridge-i egyetem pszichológiai tanszékén oktató professzor ötlete nyomán ún. személyiségtesztek segítségével „csalták ki" a felhasználóktól ismerőseik

[27] Pierre Musso: A vállalat-állam kora – avagy a politikától megfosztott politika. (Ford. Völgyes Gyöngyvér.) *Le Monde diplomatique – magyar kiadás*, 2019. július.

[28] Musso: i. m.

[29] Forgács: i. m. (2015), 70. o.

[30] Forgács: i. m. (2015), 70., 72. o.

[31] Bővebben lásd Yuval Noah Harari: *Homo Deus. A holnap rövid története.* Budapest, Animus Kiadó, 2017, 282–293. o.

[32] Frédérick Douzet: Geopolitika a kibertér megértéséhez. In Dornfeld László – Keleti Arthur – Barsy Miklós – Kilin Józsefné – Berki Gábor – Pintér István: *A virtuális tér geopolitikája. Tanulmánykötet.* Budapest, Geopolitikai Tanács Közhasznú Alapítvány, 2016, 31. o.

Facebook-profilját. „A halászat jól sikerült: 270 ezer kitöltőn keresztül 50 millió amerikai adataihoz jutottak hozzá. A Facebook erre is felfigyelt, de nem gyanakodott rá, hogy egy professzor nem tudományos célra használná az adatokat. Amikor 2015-ben megjelentek az első híradások a CA amerikai kampányban való közreműködéséről, valamint Kogan és a cég kapcsolatáról, már elkezdtek aggódni a Facebook-irodában. Először bezárták a kiskaput, majd levelet írtak a tudósnak, hogy semmisítse meg az adatokat. De ez már veszett fejsze nyele volt."[33] S bár a módszert Barack Obama csapata használta először 2012-ben, az állítólagosan elnöki ambíciókat is dédelgető Mark Zuckerberg reputációja a botrány nyomán megkérdőjeleződött – olyannyira, hogy még az amerikai kongresszus előtt is tanúskodnia kellett.[34]

A fentebb ismertetett jelenség nem független attól, hogy a mind inkább kiteljesedő globalizáció új helyzetében, az elektronikus hálózatok révén összekapcsolt, digitalizált világgazdaságban egyre több olyan funkcionális hely és intézmény létezik, amely a területenkívüliség státuszát élvezi akár a szuverén nemzetállam határain belül is. Parag Khanna érvelése szerint a 21. század térképén már nem pusztán az államokat szükséges feltüntetni, hanem a megavárosokat, vasútvonalakat, távvezetékeket, internetkábeleket, valamint egyéb, a fejlődő globális hálózati társadalmat jellemző szimbólumokat is. A komplex globális rendszer konglomerátumában a gazdaságok mindinkább integráltak, a lakosság egyre mobilisebb, a kibertér pedig összemosódik a fizikai valósággal.[35] A szuverén határokat keresztül-kasul átszövő, összekapcsolt infrastruktúrák „speciális tulajdonsággal rendelkeznek, saját életük van, több, mint egy szimpla országúté vagy távvezetéké. Határokat átlépő, megosztott igazgatás alatt működő, közös szolgáltatásokká válnak." A szállítási útvonalak, áramhálózatok, műveleti bázisok, pénzügyi hálózatok és internetszerverek a 21. századra olyan megkerülhetetlen útvonalak kifejezőivé váltak, amelyeken keresztül jelentős hatalmat gyakorolnak, és érdemi befolyást fejtenek ki.[36]

E trendekbe illeszkedik, hogy az utóbbi évtizedek rohamos fejlődése nyomán az információ létrehozása, feldolgozása és továbbítása a termelékenység és a hatalom fundamentumává, egyben fő forrásává is vált.[37] Egyes vélemények szerint az adat, az információ a gazdaság terrénumában rendkívüli mértékben felértékelődhet/felértékelődik, és a nyersanyagok szerepének csökkenésével párhuzamosan egyenesen

[33] Laky Zoltán: Beavatkozik-e a Facebook a kampányokba? Amit szabad Jupiternek... *Heti Válasz*, 2018/14. szám, 27. o.

[34] Bővebben lásd Laky: i. m. (2018), 26–28. o.

[35] Parag Khanna: *Konnektográfia. A globális civilizáció jövőjének feltérképezése.* Budapest, HVG Kiadói Zrt., 2017, 14–16. o.

[36] Khanna: i. m. (2017), 41–44. o.

[37] Manuel Castells: *A hálózati társadalom kialakulása. Az információ kora. Gazdaság, társadalom, kultúra. I. kötet.* Budapest, Gondolat–Infonia, 2005, 57. o.

a gazdasági szféra új nyersanyagává válhat.[38] Nicholas Negroponte szavaival élve a világ digitalizálódott, az atomok korát – az ipari társadalmat – felváltotta a bárhol és bármikor előállítható bitek korszaka, aminek következtében az áruk helyett a jelek továbbításának gazdaságossága vált perdöntő fontosságúvá. A digitális létezés és életmód egyre kevésbé kötődik a térhez és az időhöz,[39] és a virtuális valóság teljesen átalakítja a földrajzi határokról kialakított hagyományos gondolkodásmódunkat.[40] A hagyományos térfelfogáshoz képest a kibertér radikális nóvumot – Schmitt terminusát aktualizálva: valóságos térforradalmat[41] – jelent: tulajdonképpen egy immateriális térről van szó, amelyben a földrajzi területhez kötöttségtől függetlenül zajlanak a változások a különböző államok polgárai között, bizonyos esetekben a Formula–1-es száguldó cirkusz sebességét is megszégyenítő időbeli lefolyással, és a távolságot teljesen megszüntetve. A digitalizációnak nyilvánvaló államelméleti és geopolitikai következményei is vannak, az internet ugyanis számos geopolitikai konfliktus forrásává vált, rengeteg technikai kérdést változtatva politikai és stratégiai döntéssé. Az állami hatalom a „hálózat csapdájába" kerülve a virtuális tér számos szereplőjével szembe találja magát: bűnözőkkel, hackerekkel, aktivistákkal, nagy magánvállalatokkal, másként gondolkodókkal, az állami szférához nem tartozó szereplőkkel vagy éppen más államokkal.[42] Ezek az erőhatalmi összeütközések már nem a klasszikus geopolitikai térben zajlanak, de a geopolitikai elemzés ma sem mellőzhető, hiszen a geopolitika lépten-nyomon kísérletet tesz a kibertér meghódítására,[43] miközben a biztonsági kihívások egyre inkább totálissá válnak.[44]

[38] Csizmadia Norbert: *Geopillanat. A 21. század megismerésének térképe.* Budapest, L'Harmattan, 2016, 205, 209. o.

Ugyan nem tartozik szigorúan az általunk vizsgált témához, azonban mégis szeretnénk jelezni, hogy a klímaváltozás hatásaira – főként az emelkedő hőmérsékletre és az ugyancsak emelkedő tengerszintre – tekintettel olyan vélekedések is előfordulnak a szakirodalomban, miszerint „nem az adat, inkább a [termő]föld a jövő aranya". Simon Winchester 2021-ben megjelent *Land* című könyvének elemzésére nézve lásd Böszörményi Nagy Gergely: *Könyvek a jövőről: A termőföld a jövő aranya.* (https://bngergo.medium.com/k%C3%B6nyvek-a-j%C3%B6v%C5%91r%C5%91l-a-term%C5%91f%C3%B6ld-a-j%C3%B6v%C5%91-aranya-ba4ae9b1defe).

[39] Nicholas Negroponte: *Digitális létezés.* Budapest, Typotex Kiadó, 2002, 18, 129. o.

[40] Bővebben lásd Kelemen Roland – Németh Richárd: A kibertér fogalmának és jellemzőinek multidiszciplináris megközelítése. In Farkas Ádám (szerk.): *Védelmi alkotmányosság az új típusú biztonsági kihívások erőterében.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2018, 147–170. o.

[41] Lásd pl. Carl Schmitt: Behemoth, Leviathan und Greif. Vom Wandel der Herrchaftformen. In Carl Schmitt: *Gesammelte Schriften, 1933–1936. Mit ergänzenden Beiträgen aus der Zeit des zweiten Weltkriegs.* Berlin, Duncker & Humblot, 2021, 520–527. o.

[42] Erre nézve bővebben lásd Kelemen Roland – Németh Richárd: A kibertér alanyai és sebezhetősége. *Szakmai Szemle*, 2019/3. szám, 95–118. o.

[43] Douzet: i. m. (2016), 22–23. o.

[44] Lásd Farkas Ádám: A totális államtól a totális háborún át a totális védelemig. *MTA Law Working Papers*, 2015/34. szám; Farkas Ádám: *A totalitás kora? A 21. század biztonsági környezetének és kihí-*

A szuverenitás kinyilvánítására egyébként az információs tér képviselői is kísérletet tettek; John Perry Barlow 1996-ban „képernyőre vetette" a virtuális tér függetlenségi nyilatkozatát. „Gondos és jó alapító atyaként" azt is deklarálta, hogy a kibertér saját szuverenitással rendelkezik, megtoldva mindezt azzal a rendelkezéssel is, miszerint az „intellektualitás civilizációja" mentes az állami szervek által megalkotott jogszabályok hatálya alól. Alix Desforges mindehhez azt tette hozzá, hogy a hálózat a nyitottság, az önirányítás, a szabad információáramlás és a szólásszabadság „terepe", és a hagyományos állami hatalomhoz képest erősen decentralizált, illetőleg központ nélküli.[45]

A kibertér önjelölt prófétáinak eme megnyilvánulásaival szemben a különböző államok döntéshozói természetesen igényt kívánnak formálni a virtuális tér „regulák közé szorítására". Az államok argumentációjában a virtuális tér felügyelet és ellenőrzés alá helyezendő, kvázi uralom alá hajtandó „*res nullius*-ként" tűnik fel; ennek legitim indokaként a legtöbbször a nemzetbiztonsággal szembeni fenyegetéseket, valamint a nemzeti érdeket jelölik meg. Hozzá kell tenni ugyanakkor, hogy az egyének védelme is legalább ennyire legitim módon szükségessé teszi az állami jelenlétet; ezt indokolják az egyéni adatokra irányuló kibertámadások, hiszen az ezek révén okozott károk egyes esetekben akár a millió dolláros tételeket is elérhetik. (A cégek, vállalatok esetében pedig 100 millió, sőt akár milliárd dolláros összegekre rúgó károkról is lehet hallani.[46]) Az egyre gyakoribbá váló kibertámadások nyomán mind több és több állam ismeri fel a kapacitások megerősítésének szükségességét, és az állami hatalom „információs szupersztráda" feletti kontrolljára vonatkozó igényét. A francia védelmi minisztérium korábbi köztisztviselője, Stéphan Dossé alighanem fején találta a szöget, amikor deklarálta, hogy „az államoknak fel kellett húzniuk a zászlót a kibertérben, amit elfoglalnak, és ahol szuverenitásukat gyakorolják, hogy a szűzföldeket gyarmatosítsák, és felkészüljenek egy esetleges támadásra".[47] Az információs és kommunikációs rendszerek végeláthatatlan terjeszkedésének ugyanis stratégiai tétje van, ezért az államoknak minél gyorsabban és hatékonyabban reagálniuk kell a kibertér jelenlétéből következő kihívásokra. Az információk gyűjtése, elemzése, kézben tartása – adott esetben manipulálása –, továbbá a megfelelő védelmi kapacitás kiépítése és fejlesztése prioritást kell, hogy élvezzen az államok számára. Ez a munka pedig már meg is kezdődött: a magánszféra egyes szereplői mellett az államok is „elkezdték birtokukba venni a kiberteret és az adatokat. Így az érdekelt felek különböző geopolitikai következményeket észlelhetnek, akár az általuk gyakorolt politikai vagy jogi ellenőrzés, akár az abból általuk merített erőforrások,

---

vásainak totalitása és a totális védelem gondolatkísérlete. Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2018.

[45] Douzet: i. m. (2016), 27. o.

[46] Lásd Danyiil Turovszkij: *Orosz hekkerek. Így lettek lázadókból Putyin katonái.* Budapest, Athenaeum, 2020.

[47] Douzet: i. m. (2016), 28. o.

akár az általuk kivetített értékek és szimbólumok vagy a rájuk áthárított azonosítási folyamatok terén. Végső soron e különböző – helyi, nemzeti, regionális szinteken – végbemenő territorializációs dinamika versengési és hatalmi viszonyok kialakulását vonja maga után a kibertérben, számos játékost mozgásba hozva."[48]

De miként is tudjuk tipizálni a kibertérben érvényre juttatott egyéb – alapvetően államifeladat-kifejtéssel kapcsolatos – tevékenységeik karakterisztikája alapján az egyes államokat? A Kelemen által közzétett, korábban is idézett tanulmány ebben is a segítségünkre lehet, hiszen a cyberfare state-tel kapcsolatos fogalomalkotás, valamint tipizálás folyamán különböző alcsoportokat (vagyis az ő megfogalmazásában almodelleket) állított fel. A hatalmi állam ideáján és gyakorlatán felépülő (orosz, kínai, szingapúri, egyes aspektusokban észak-koreai) almodelljében „a kibertérre támaszkodó technológiai újításokon nyugvó szociális, jóléti intézményeket, végső soron [a] szolgáltató közigazgatás javítását, modernizálását társítják a totális kontroll és adatok feletti totális rendelkezés lehetőségével, amelyekhez sok esetben támogató potenciál kiépítése kapcsolódik. A *cyberfare state* ezen hatalmi jellegű attribútumokat felmutató államokat a fentiek okán *smart total control cyberfare state*-nek nevezhetjük."[49]

Ezzel áll szemben a nyugati államok almodellje, amely főleg a digitalizáció jóléti reformjára fókuszál, átalakítva a szolgáltató közigazgatást, nagy volumenű innovációt mutatva fel az oktatás, a kutatás és az egészségügy terrénumaiban, olyan projekteket indítva útjára, mint az okosváros-programok, az önvezető gépjárművek vagy az MI-programok. Ez az almodell természetszerűleg teljesen más filozófia mentén szerveződik. „Ebben a közegben elképzelhetetlen volna az egyén, vagy akár a gazdasági szereplők feletti felügyelet még közel hasonló szintjének kialakítása is, mint amit Kínában láthattunk. A kontrolleszközökön túl, a kibertérhez való hozzáférés korlátozása sem képzelhető el olyan mértékben, mivel egyes államok egyenesen alapjogként tekintenek az internethez való hozzáférésre, de más államok esetében is garanciák garmadája védi ezt."[50] A transzatlanti térségben tehát a *cyberfare state* úgy munkálható ki, hogy közben szavatolni kell a jogállam alapvető összetevőit és biztosítékait (hiszen a modern nyugati civilizáció domináns állammodellje köztudomásúlag a liberális állam eszményéhez kapcsolódik),[51] „de mindeközben meg

[48] Amaël Cattaruzza: *A digitális adatok geopolitikája. Hatalom és konfliktusok a Big Data korában.* Budapest, Pallas Athéné Books, 2020, 52–53. o. Idézi: Farkas Ádám: Biztonság – Geopolitika – Digitalizáció, avagy Amaël Cattaruzza „A digitális adatok geopolitikája" című kötetének főbb üzenetei. *Smart Law Research Group Working Paper*, 2021/1. szám, 5. o. A „virtuális geopolitika" egyes aspektusaira nézve lásd továbbá Abishur Prakash: *Új geopolitika. A világ jövője. Technológia.* Budapest, Pallas Athéné Könyvkiadó Kft., 2018, 141–151. o.

[49] Kelemen: i. m. (2022), 13. o.

[50] Kelemen: i. m. (2022), 15. o.

[51] Pócza Kálmán: *Álmaink állama. Egy hatalmi centrum az ezredfordulón.* Budapest, Századvég Kiadó, 2002, 138. o.

kell teremteni a biztonsággal való egyensúlyt".[52] E megállapítást osztva kiemeljük: tudomásul kell vennünk, hogy az intenzív technológiai fejlődés az államot és annak polgárait is újszerű biztonsági kihívások elé állította, és a szabadság versus biztonság komoly múltra visszatekintő dilemmájában – a *protego ergo obligo* hobbesi eredetű elvének is betudhatóan[53] – sokan éppen a biztonság szavatolását tartják prioritásnak. A *co-operating cyberfare state* számunkra is irányadó almodelljében az együttműködés kiindulópontja szintén a jóléti-szociális digitalizáció, de a felek között egy olyan legjobb gyakorlatot kell kialakítani, amely a jogállami garanciákat tiszteletben tartva, de mégis a biztonság hatékonyságát favorizálja. E *best practice* magában foglalná az állami szereplők (civil és katonai karakterű szervek) tapasztalatait, elvárásait és teoretikus megközelítéseit, illetve a gazdasági szereplők ugyanezen szempontjait, kutatói-innovációs oldalról pedig a társadalomtudományok, a hadtudomány és a műszaki tudományok reprezentánsait.[54]

***

Navigare necesse est, vivere non est necesse, azaz *hajózni muszáj, élni nem* – hangzott el a Szicíliából Rómába gabonát szállító hajósokat „feltüzelni kívánó" Nagy Pompejus verdiktje. Nos, e formula első felével minden további nélkül azonosulni tudunk – az egyre gyakrabban globális hatókörű örvények áramlatai között is szükséges ugyanis a megfelelő navigáció –, főleg, ha elfogadjuk, hogy a globalizáció a különféle hálózatok és áramlások terjedése révén „a tenger logikájához kapcsolódik, amely nem ismer el határokat vagy zárt területeket".[55] A globalizáció óceánjának erejét természetesen nem becsülhetjük alá, ugyanakkor azt is el kell fogadnunk, hogy világképünket továbbra is a nemzetek hajói uralják.[56]

[52] Kelemen: i. m. (2022), 17. o.

[53] Bővebben lásd Carl Schmitt: A politikai fogalma. In Schmitt: *i. m.* (2002), 35. o.

[54] Kelemen: i. m. (2022), 18. o.

[55] Alain de Benoist: *Carl Schmitt Today. Terrorism, 'Just' War, and the State of Emergency*. London, Arktos Media Ltd., 2013, 105. o.

[56] Utalás Muraközy László metaforájára. Lásd Muraközy László: *Az államok kora. Az európai modell*. Budapest, Akadémiai Kiadó, 2012, 295. o.

SIMON LÁSZLÓ

Az egyén mint nem állami szereplő a kibertérben megjelenő fenyegetési palettán, avagy a kiberpartizán kérdése

„...bellum omnium contra omnes"
Thomas Hobbes (1642)[1]

Az emberi kapcsolatok növekvő számú és egyben legbonyolultabb viszonyrendszerét éljük. A tanulmány e rendszer modern interakcióinak azon alkotórészét igyekszik analizálni, amely a közösségi párbeszéd hagyományos eszközeit és módszereit, valamint a forradalmi újításokat előidéző infokommunikációs találmányokat és innovációkat azonnal alkalmazni igyekszik. Az alterület növekvő jelentősége abban mutatkozik meg, hogy az elektronikusan, digitálisan összekötött egyének, a virtuális felhasználók a közhatalom megosztásával, átruházásával közvetve kapcsolódnak ugyan egy-egy államhoz, de nem állami szereplőként – még az adott ország állampolgárának sem kell lennie –, mégis képesek lehetnek önálló politikai akaratuknak érvényt szerezni, közösségeket vagy más állami szereplőket befolyásolni. Az össztársadalmat alkotó egyénekhez kötődő egyedi aktivitás vizsgálatával az erő és erőkivetítés legkevésbé sem újszerű fenyegetése is azonosítható, amely közvetett módon, de érdemi fenyegetést jelent az adott kormányzat tevékenységére. A demokráciák belső működését szolgáló társadalmi szerződés és az államok együttműködését, illetve konfliktusainak rendezését biztosító nemzetközi megállapodások olyan kihívások előtt állnak, amelyek az arctalan agressziót és nem utolsósorban anómiás állapotot eredményezhetnek, illetve szándékosan – hatalmi és gazdasági szempontokat előtérben tartva – azt tartanak fenn. A 21. században eddig kialakult válságok és a növekvő számú problémás helyzetekben a megoldást hagyományosan szolgáló hierarchikus hatalmi felfogás, illetve a tradicionális társadalmi diskurzusok inkább elmélyítették a konfliktusokat, mint feloldották azokat. A világunk ütközőzónáiban a békét ideig-óráig vagyunk képesek kikényszeríteni, fenntartani, és egyre inkább szembesülünk azzal, hogy a mesterségesen

[1] Hobbes a *De Cive* (magyarul: A polgárról) című művében fogalmazta meg, hogy a polgári társadalom nélkül, vagyis pusztán természeti környezetben minden embernek joga van háborúzni a másik emberrel. „A mindenki háborúja mindenki ellen" felfogást Hobbes az 1651-ben befejezett (1668-ban angolul *Leviathan or The Matter, Forme and Power of a Commonwealth Ecclesiasticall and Civil* címmel megjelentetett) művében az emberi létet már a versengő, küzdő, háborúzó emberek közösségeként írta le. A gondolatkísérlete a társadalmak szerveződésének gyakorlatával, illetve a legitim kormányzás elméletével foglalkozott. – Thomas Hobbes: *Leviatan I–II.* Budapest, Kossuth Kiadó, 1999, 652. o.

létrehozott és támogatott állami struktúrák nem képesek vagy nem érzik sajátjuknak a nyugati típusú, modern demokratikus társadalmi[2] felfogást. Ezt pedig az infokommunikációs robbanásból következő államszervezeti, szabályozási és biztonsági hatások tovább fokozzák. Ez természetesen kihat a politikai-társadalmi berendezkedésre és működésre is, valamint azokra a keretekre, amelyek között az egyének érdekeik érvényesítésére akár közösségi léptékben is törekedhetnek.

A 17. századi mottó olyan evidenciára utal, amelyet az emberiség a kapcsolatokból eredő verbális és fizikális erőszak révén folyamatosan fenyegetésként él át. Az emberi társas viszonyok generálisan hordozzák az élethez és önvédelemhez kötődő egyéni jogot, és az ebből közvetlenül levezethető agresszió jogát. Leegyszerűsítve ebből fakad a konfrontációk elkerülésének közösségi kötelezettsége és a legitim háborúk viselésének joga is. Értékelésem szerint a történelemben visszatekintve Hobbes gondolatai – korának megfelelő filozófiai és politika- jogelméleti megközelítése – kétségtelenül olyan társadalmi konfliktusra igyekezett rávilágítani, illetve megoldást keresni, amely később az 1642 és 1651 közötti angol polgárháborúban csúcsosodott ki. A „mindenki háborúja mindenki ellen" üzenete azt az örök érvényű jelzést, figyelmeztetést is magában hordozza, amely szerint az emberi kapcsolatokban rejlő fenyegetések – azok szociális, kulturális összefüggései és nem utolsósorban a párbeszéd helyéül szolgáló természetes és mesterséges környezet – társadalmi szabályok jogok és kötelezettségek, követelmények és retorziók nélkül agresszióhoz, konfliktusokhoz, szélsőséges esetekben az erőszak spiráljához vezetnek.

1. A VILÁGREND BIZTONSÁGI HÁLÓJA A BIZTONSÁGOS HÁLÓZATOK VILÁGRENDJE

A 21. század kapcsolatait egy látszólag átgondolt, a kapcsolódások alapjául szolgáló információs kötődések miatt valamiféle McLuhan-i globális faluban[3] igyekszünk értelmezni. Bár McLuhan kulturális megközelítése, miszerint az 1960-as évek elején

[2] A tanulmányban a társadalmi felfogást sem filozófiai, sem szociológia értelemben nem kívántam leegyszerűsíteni. Az egyéni aktivitás és a társadalmi viszonyokra fenyegető hatása mindenképpen jogfilozófiai és társadalomelméleti, értékszociológiai összefüggésekben nyernek értelmet. Távol maradva a nyugat-európai demokráciák fejlődéstörténetének legújabb címkézett vitájától, sem a liberális, neoliberális, sem pedig az „illiberális", autokrata, populista felfogású modern demokráciákkal nem tisztem foglalkozni. Korunk hatalmi rendszerét és folyamatosan változó hatalmi alrendszereit a jelenlegi demokratikus intézményrendszer működése és a kormányzáselmélete szempontjából elemeztem. Tehát jelen változó és a szó eredeti értelmében „korcs", „parázna" hibrid társadalmi helyzetekben a nyugati típusú modern demokrácián, annak alapdokumentumokban rögzített közösségi érdek és érték viszonyrendszerét, az állami intézmények alkotmányos működését és a közhatalom modern megvalósulását érthetjük. Vö. Cs. Kiss Lajos: A szociológiai rendszerelmélet államfelfogása. *Jog Állam Politika.* 2010/3. szám, 3–34. o.

[3] Vö. Marshall McLuhan: *A Gutenberg-galaxis.* Budapest, Trezor Kiadó, 2001, 332 o.

tapasztalható technológiai vívmányok új információmegosztó képességeire támaszkodott, a rádióhullámok és a televíziózás mint a valóságot hitelesen leképező technológia még nem volt elég fejlett ahhoz, hogy életében kiteljesítse a társadalmi vízióját. Ebben az időben a beérett szabadpiaci folyamatok globális gazdasági hatását egy térben és időben összekapcsolt hálózatba átképezve hasonló szabályozó rendszer elterjedését jelentette, de már politikai, szociális, kulturális és egyéb tekintetben is.[4] A békés, barátságos – infokommunikációs értelemben azonos, egyenértékű – polgárok, felhasználók közössége eleinte technikai értelemben, később pedig már más társadalmi összetevők miatt sem alakulhatott ki.[5] Az információk matematikai, logikai értelmű objektivitásából vagy az általuk hordozott adatok, tények neutrális jellemzőkből fakadó – sérülésektől és zavaroktól mentes és hibajavíthatósággal bíró – technikai és logikai hálózatok még ma sem érhetők el. A szabadpiac szereplőihez, illetve a fogyasztókhoz kapcsolódó érték- és érdekrendszerekben az elmúlt 30 évben meghonosodott emberi viselkedési típusokat és viszonyokat (pl. az értékesítési láncokban a termelő a fogyasztó és a kereskedő is jól jár, vagy a kereslet és a kínálat határozza meg a termékek árát, stb.) tekintve, minden szereplő közös törekvése ellenére az „üzembe helyezett" modern információs hálózat, az internet sem tudta elérni a teljes gazdasági pluralizációt.[6] Épp ellenkezőleg! Ahogy Castells kutatásai és a sok évig folytatott tudományos vitái előrevetítették, nemcsak a technológiától való

[4] Z. Karvalics László: Marshall McLuhan helye az információs társadalom elmélettörténetében. *Replika,* 2011/3. szám, 25–33. o.

[5] Könnyen belátható, hogy az információ és a tényszerű adatok azonos észleléséből nem következik az azonos megítélés vagy az egyetemes törvényszerűség sem. A matematika a logika vagy az ekvivalencia révén alkalmas például objektív és axiomatikus evidenciák igazolására, vagy jelenségek és tulajdonságok okainak, valamint determinált következményeinek bizonyítására. Ahogy azt Fukuyama megfogalmazta, olyan identitás jelent meg a felhasználók között, amely nemhogy egyformává tette a földrajzilag elkülönülő infokommunikációs társadalom tagjait, hanem új minőségű, követendő, de ugyanakkor megosztó személyiségeket (nevezzük influenszereknek őket) formált meg: „In contemporary societies, these social changes were deepened by modern communications technology and social media, which allow likeminded individuals in geographically separate places to communicate with one another. In such a world, lived experiences, and therefore identities, begin to proliferate exponentially, just like YouTube stars and Facebook circles on the internet. What erodes just as rapidly is the possibility of oldfashioned »experience,« that is, perspectives and feelings that can be shared across group boundaries." – Francis Fukuyama: *Identity – The Demand for Dignity and the Politics of Resentment.* Farrar, Straus and Giroux, New York, 2018.

[6] „A gazdasági pluralizmus – szűkebben a piaci pluralizmus – a gazdasági élet érdekpluralizmusát, az érdekek sokféleségét és versengését, a piacon versengő autonóm vállalkozók sokféleségét jelenti. Klasszikus a szabad versenyes doktrína, amely mai formájában a politikai pluralizmus egyik tartópillére. Innen ered az a felfogás, amely a gazdasági szféra privát autonómiáinak a korlátozásában, a magántulajdonosi önállóság és az ezen alapuló gazdasági, vállalkozói autonómia és szabadság megszüntetésében a politikai pluralizmus alapjának a felszámolását látja (Hans Kelsen, Gustav Radbruch, Rudolf Stammler). A kritika éle a fasiszta és a szocialista országok korlátozott magántulajdona és erős állami beavatkozása ellen irányul. A magántulajdonon és az autonóm vállalkozók versengésén alapuló gazdasági pluralizmus teremti meg a politikai pluralizmus lehetőségét." – Bihari Mihály: *Politológia*

félelem okozhat frusztrációt a hálózathoz csatlakozókban, hanem az információs társadalmak paradigmájában foglalt információs és technológiai konvergenciákból következő identitás- és értékátalakulások[7] is félelemkeltőkké váltak.

A II. világháborút követő időszak szocialista és kapitalista érték- és érdekrendszere 1991-ig a világrend két pólusát alakította ki. A társadalmi ideológiák által kialakított és arra alapuló, két hierarchikus gazdasági felfogás szerint az erőforrásokat a két hatalomcentrum, az USA és a Szovjetunió birtokolta. A hatalmi struktúrákat ugyan földrajzi és fizikai értelemben is vasfüggöny határolta, a tervezetten folytatott gazdálkodás a hangzatos eredmények és hosszú távon is rendelkezésre álló nyersanyagok és energetikai erőforrások ellenére a 20. század végére már nem szolgálta a kommunista ideológia elterjedését, és a gazdasági növekedéshez szükséges technológiák megújítását. Leegyszerűsítve a szocialista állampárti közösség belső gazdasági reformjai nem az elszigetelést, hanem a „piacgazdaság szellemének" elterjedését és a pártállamok európai jelenlétének végét eredményezte.[8] A bipoláris hatalmi rendszer megakadályozta egy újabb világméretű fegyveres konfliktus kibontakozását, azonban a helyi és a regionális összetűzések (pl. ideológiai, politikai, gazdasági vagy akár katonai eredetű) e világrend hatalmi mechanizmusaiban is jelen voltak, de a totális szembenállás elkerülésére fókuszáló biztonsági érdekek szerint kezelve. Tehát a fennálló hierarchikus hatalmi rend még ha sok esetben véglegesen nem is tudta feloldani az ellentéteket, vagy biztonságosan konzerválta a szembenállást egy időre, vagy lényegesen egyszerűbbre változtatta azt.[9] Bár a konfliktusok euroatlanti közel-

– *A politika és a modern állam. Pártok és ideológiák.* Budapest, Nemzedékek Tudása Tankönyvkiadó, 2013, 204. o.

[7] Lásd Hendlein Teréz – Prazsák Gergő: A hálózati társadalom receptje. *Információs Társadalom,* 2005/4. szám, 130–138. o.

[8] Gorbacsov nevével jelzett Glasznoszty és Peresztrojka jelentősége és az 1989-es máltai csúcson elhangzottak, de dokumentumokkal nem deklarált ideológiai és tartalmi elemei mai napig megosztják a posztszovjet térség gondolkodóit és elemzőit, a hidegháború és a vasfüggöny végét, valódi szabadságot, felszabadulást jelentették a pártállamok polgárai számára. Bővebben Vaszari Tamás: *Oroszország geogazdasági és geopolitikai dilemmái a XXI. század elején, valamint ezek történelmi előzményei.* Győr. Széchenyi István Egyetem. Doktori értekezés, 2018. Ezt még akkor a világ biztonságát jelentősen pozitívan befolyásoló világeseményként kell értékelni, ha a tanulmány írásakor, 2022-ben a február 24-én megindított ukrajnai orosz fegyveres invázió (orosz–ukrán háború vs. orosz különleges műveletek) közepette és Gorbacsov 2022. augusztus 30-i halálát követően egyre többen a reformokat okolják a posztkommunista országok nemzeteinek, kisebbségeinek fegyveres konfliktusai miatt. Ahogy Alekszej Venediktov orosz újságíró fogalmazott: „All of Gorbachev's reforms are now zero, in ashes, in smoke!" (*Gorbacsov reformjai most semmivé, hamuvá és füstté váltak!* Lásd: Anton Troianovski: With War in Ukraine, Putin Tries to Unravel Gorbachev's Legacy. *The New York Times*, 2022. 08. 31. (https://www.nytimes.com/2022/08/31/world/europe/gorbachev-putin-russia.html); Forbes Talk, *Youtube* (https://www.youtube.com/watch?v=GRGfcFJCdI0).

[9] Például a koreai, a vietnámi vagy az afganisztáni vagy az angolai, a mozambique-i, a csádi, az etiópiai és az észak-jemeni polgárháborúk lezárása afféle „békés megoldást" jelentettek a térség lakosainak, de nem minden esetben sikerült olyan működőképes kormányzatot hátrahagyni, amelyek a nemzetkö-

sége és azok globális, valamint regionális szintű fenyegetése Moszkva és Washington legmagasabb aktivitását és elhúzódó fegyveres összetűzéseket eredményezett, az agressziót elszenvedők mások segítségére nem számíthattak. A két hatalmi pólus gazdasági, szociális, társadalmi és nem utolsósorban információs erőkivetítése, befolyásolása gyakran hordozták az érdemi változások ígéretét, de 1953 és 1982 között a Német Demokratikus Köztársaságban, Magyarországon, Csehszlovákiában vagy Lengyelországban nem avatkozott be a NATO, csak verbális szinten, a Szovjetunió pedig közvetlenül katonai erővel és közvetett módon a helyi politikai elit segítségével birtokolta a hatalmat.

A Szovjetunió felbomlása utáni világrendet és fenyegetéseit vizsgálva a közhatalmat demokratikusan gyakorlók és egyéb hatalmat birtokolni kívánok figyelmét a világpolgárok és állampolgárok képviseletének kérdéskörét már nem csak az értékek és érdekek tradicionális viszonya határozza meg. A hatalommal közvetlenül és közvetve összefüggő információk terjesztésének és terjedésének, illetve a megválasztott felhatalmazott vezetés hatalmának kiteljesedése már nem az ideológiák által sulykolt értékek és az abból logikailag levezetett érdekek rendszerén alapul csak. Az információs társadalmak együttélését a két 20. századi dogmatikus stratégia nemcsak a sikereik és kudarcaik miatt nem határozhatja meg, hanem azért sem, mert a 21. században egyre többen ismerik fel, hogy az ideológiák hangzatos tartalamainak ellenére „az érték nem létező, nem valóságos, hanem érvényes".[10] Az ideológiák és az általuk kijelölt például huntingtoni civilizációk[11] különböző forrásokból (gazdasági, vallási, kulturális stb.) származó érdekellentétei törésvonalakat hozhatnak létre. Felvetésem szerint a jelenkorunk hatalmi rendszere a globalizáció hatására igyekszik egy tégelyben felolvasztani a történelmi gyökerekkel rendelkező állami szintű közösségek kulturális és szociális különbségeit. Ugyanakkor a már említett vagy azon túl, újonnan „feltalált" vagy „kitalált" törésvonalak esetében – különösen a határterületeken – folyamatosan szembenállást, a földrajzi leképezhetőség esetén

---

zi támogatások felhasználásával képesek lettek volna hosszú távon fenntartani a polgáraik biztonságát. Lásd Lowe (2021). A több országot érintő közel-keleti arab–izraeli fegyveres konfliktusok, vagy az iraki, szíriai háborúk esetében szemben álló feleket is a „hidegháború alatt a közel-keleti országokat a két szuperhatalomhoz fűződő kapcsolataik alapján gyakorlatilag egy »nyugati« és egy »keleti« blokkhoz lehetett sorolni". – Selján Péter: A közel-keleti hatalmi egyensúly átalakulása. *Nemzet és Biztonság – Biztonságpolitikai Szemle*, 2016/4. szám, 30. o.

[10] Cs. Kiss Lajos: Alkotmányelmélet és az érték logikája: zsarnokság vagy szabadság? *Jog Állam Politika*, 2017/3. szám, 11. o.

[11] Huntington érvelése szerint az információs társadalmak korának konfliktusait alapvetően nyugati szövetséges keresése, illetve megnyerése dönti el: „a Nyugat az egyetlen civilizáció, melynek számottevő érdekeltségei vannak az összes többi civilizációban vagy térségben és képes befolyásolni az összes többi civilizáció vagy térség politikáját, gazdaságát és biztonságát. Más civilizációk társadalmainak rendszerint szükségük van a nyugati segítségre, hogy elérjék céljaikat és megvédjék érdekeiket." – Samuel P. Huntington: *A civilizációk összecsapása és a világrend átalakulása.* Budapest, Európa Könyvkiadó, 2006.

pedig fegyveres konfliktusokat eredményeztek, eredményeznek. A társadalmi párbeszédek és szerződések (alkotmányok és alaptörvények), az állami, vagy magasabb szintű szövetségesi megállapodások ellenére vannak egyének és csoportok, amelyek nem adják fel függetlenségi és hatalmi törekvéseiket. Úgy folytatták morálisan és erkölcsileg megosztó tevékenységüket, nem egy esetben fegyveres harcukat, hogy az egyes felek eltérő nézőpontjából legitim szabadságharcot vagy szélsőségesen illegitim terrort folytassanak. Az elmúlt húsz évben folytatott számtalan kutatás és nyomozás eredményeként az al-Káida terrorszervezet akciójaként azonosított cselekmények – 2001. szeptember 11-én egy kis csoport által összehangoltan végrehajtott amerikai terrortámadás – (a továbbiakban: 9/11 eseménye) után tett nemzetközi erőfeszítések a többek által hangoztatott és többek által tagadott vagy ki nem mondott egypólusú, amerikai központú világhatalmi törekvés[12] egyik alappillére volt. Az általam korábban[13] anyagcentrikus hadviselési kultúraként azonosítható válságkezelő metódus, a nyugati típusú, globális technikai-gazdasági szemléletű hatalmi források birtoklásának megközelítése, ahogy azt Rostoványi 2002-es kutatásai előre jelezték, az erőszak öngerjesztő ciklusává vált.[14] A globalizáció és az infokommunikációs hálózatok technológiai előnyeit felhasználva a nyílt társadalmi (Open Society) hálózatok jelentek meg. Az elsősorban közösségi igényre hivatkozva és tudományos érvelés mellett, ugyanakkor „első vagy második blikkre" gazdasági megfontolások alapján létrejött közösségi mozgalmak természetvédelmi, egészségügyi, kulturális és egyéb szociális célokat hirdetve építették cselekvő és támogatói csoportjukat. A látszólag pénzügyileg független csoportok az önkéntesen kijelölt és a közösség érdekére hivatkozva a kijelölt aktivitási területeken az esetenként erőszaktól sem mentes cselekményeik hatása az államok és kormányok szerepét, illetve annak jelentőségét nemcsak képletesen csökkentették. A kormányzatok közvetlen állampolgári információs kapcsolatait folyamatosan szűkítve, az állami irányítási és vezetési folyamatok, de még a szabályozás tekintetében is alternatív megoldásként, a kormányzati bürokráciánál aktívabb és hatékonyabb érdekérvényesítést, konfliktuskezelést értek el. Az egyes kormányokon túlmutatató, vagy multilaterális kormányzati együttműködést igénylő témakörökben, de a társadalmi és szociális problémák megoldásában is olyan tudományos műhelyek (think tankek) és nem állami vagy civil szervezetek (angolul: non-governmental organisations, a továbbiakban rövidítve: NGO-k) jelentek meg, amelyek kommunikációjuk és tevékenységük révén közvet-

[12] A bipoláris hatalmi világrend megszűnését követő, illetve azt okozó gazdasági modell azt a feltételezést erősítette, hogy az emberi kapcsolatok más területein is sikeres lehet azon hierarchikus rendszert alkalmazni, amelyet a Pax Americana világformáló gondolatvilága testesített meg.

[13] Simon László: Az információ mint fegyver? *Szakmai Szemle*, 2016/1. szám, 34–60. o.

[14] Rostoványi Zsolt: Civilizációk a civilizáció ellen? A hidegháború utáni nemzetközi rendszer antinómiái. *Külügyi Szemle*, 2002/1. szám, 39–72. o.

ve vagy közvetlenül tudtak hatást gyakorolni az államok hatalmi alrendszereiben.[15] A hatalmi rendszer hierarchiáját fenntartó anyagi tényezők mellett megerősödött a közösségi, egyéni kapcsolatok rendszere. Így pontosan az információk megosztásán alapuló eszmei és öntudatos, vagyis kulturális és szociális elemek által meghatározott cselekvő hálózatok alakultak ki. A Rostoványi által interdependens nemzetközi rendszernek nevezett közegben az – alapvetően lokális és regionális területeken létező, kialakuló – egyének és a közösségek közötti ellentéteket is figyelembe kell venni.[16] Ma már a „modernizáció centrumát alkotó polgárok jogos és racionális elvárásai, amelyek az ellenséges fegyveres tevékenységek felszámolását eredményezhetné, azok váltak az újabb erőszak kiindulópontjaivá. A globalizáció és a modernizáció jelenleg kibontakozóban lévő szabályozottság tekintetében még kevésbé bürokratikus, és az egyes államok hatalmi szempontjai alapján egyénileg még kevésbé uralható, vagy csak együttműködésben kezelhető gazdasági perifériákon (a kibertérben, a mesterséges intelligencia forradalma, a nemzetközi űrpolitika fejlődése, vagy a nemzetközi és az édesvizeink felhasználása és megosztása, a nanotechnológia vagy a genetikai beavatkozások alkalmazása stb. terén) megjelenő érdekérvényesítés során nem állami hatalmi aktivitás jelezhető előre. A hálózati szereplők és az államok hierarchikus hatalmi rendszerében a „későbbiekben kibontakozó erőszak joga tehát a válságok esetében öngerjesztő terror-spirált eredményezhet".[17]

2. AZ EGYÉN/FELHASZNÁLÓ MINT NEM ÁLLAMI HATALMI SZEREPLŐ AZ INFORMÁCIÓS TÁRSADALOMBAN

Abban a realisztikus elképzelésben éltünk, miszerint a világbéke és a globalizáció talán legsikeresebb alrendszere, a világgazdasági rendszer szabad pénzügyi piacainak törvényszerűségei, önszabályozó mechanizmusai életünk egyéb területein is, azaz generálisan alkalmazhatók. A matematikai szabályok és egyéb attribúmások több száz éves tapasztalatai, a kereslet-kínálat által nyújtott modell nemcsak pénzügyi, de szociálpszichológiai fékeinek és ellensúlyainak rendszere kialakítható

[15] A legismertebb és leghatékonyabb csoportosulásuk között szerep a Greenpeace, a World Wide Fund for Nature (WWF), a Médecins Sans Frontières (Orvosok Határok Nélkül), de a Magyarországon is jelentős kormányzati befolyásolásra törekvő Transparency International vagy az Amnesty International is NGO.

[16] A „fő törésvonalak, konfliktusforrások elsősorban nem a különböző civilizációk, illetve kultúrák között, hanem egyre inkább a(z egyes számú) civilizáció és a (többesszámú) civilizációk, illetve a(z egyes számú) kultúra és a (többes számú) kultúrák között fognak húzódni, illetve húzódnak már ma is". – Rostoványi: i. m. (2002), 40. o.

[17] Simon László: A válságkezelés során felhasználható nemzetbiztonsági információk katonai oldala. Orbók-Barkovics Veronika – Orbók Ákos: *A hadtudomány és a XXI. század 2018.* Budapest, DOSZ Hadtudományi Osztály, 2018, 251. o.

korunk információs társadalmi hálózataiban is. A tudatos egyén az összekapcsolódó infokommunikációs eszközök segítségével, a közösségi média által közvetített és rögzített tartalmakból tájékozódva az információ kereslet-kínálati szabad piacán békésen lesz képes együttműködni, vagy akár közvetlenül kereskedni az információval, közvetetten pedig bármivel, amelynek tartalmi képe és értéke leképezhető a kibertérben. Már Castells is előrevetítette, hogy az internet fejlődésével kialakulhat az a hálózati társadalom, amely az államok beavatkozása nélkül, önálló közösségi szabályai lapján létezik és fejlődik. Castells felvetése szerint a felhasználónak, mint a hálózati társadalom individuális alapkövének – az infokommunikációs hálózatok nyújtotta kapcsolati rendszerben – nincs szüksége az állami szerveződési szintre. Hasonlóan az NGO-k gazdasági, vagy más társadalmi és szakpolitikai tevékenységéhez, az egyének globális szerveződése – a szabadpiaci szabályokkal hasonlatos elvek mentén – akár állami beavatkozás nélkül is működőképes. Bár maga Castells szociális megközelítése gazdasági alapokra épül, viszont ő maga is megfogalmazza a rendszer frusztráló kulturális hatásait, és annak konfliktusokkal terhelt folyamatait, a személytelen rendszer alkalmazásának negatív következményeit.[18]

Az elmúlt harminc évben a nyugati demokráciák egyéni és közösségi értékeik és érdekeik globális kiterjesztését eddig még soha nem tapasztalt méretekben és mélységben igyekeztek megvalósítani. A bipoláris hatalmi helyzet megszűnését felhasználva a korábbi földrajzi sokszínűséghez kapcsolódó kulturális és szociális különbségeket is igyekezett egyenarcúsítani, multikulturálissá fejleszteni. A valós idejű, uralkodó közösségi média a piaci trendek sugárzásával képessé vált feloldani a generációs és egyéb kulturális és szociális különbségeket. A társadalmi sokszínűség jelentősége felületessé vált. A nyugati demokráciák egyik fundamentumának, a másság elfogadásának központi „követelménye" ellenére, a vezető infokommunikációs trendekkel azonosulni nem tudók elszigetelődnek. A szociálpszichológiai hatások mélyebb elemzése nélkül is belátható, hogy a kibertérben kibontakozó mesterséges intelligencia piaci jellegű alkalmazása például nem csak technikailag képes feloldani, de el is tünteti az anyanyelvi gondolkodásban mélyen gyökerező ön- és társastudat morális közösségét. A logaritmus a felhasználó egyedi elektronikusan azonosított kompetenciája alapján keres és ad személyesnek tűnő válaszokat. De ennek következményeként értelmezhető az azonos identitástudatból fakadó és a fizikai kontaktusra, kinetikus beavatkozások lehetőségére épülő biztonságérzet csökkenésének kérdésköre is. Az infokommunikációs rendszerek alapvetően globális fogyasztásra hangolt üzenetei algoritmizált folyamatok eredményeként, másolandó sémaként jelennek meg. Az interneten jelen lévő közösségi megosztások a biztonság fenntartásának olyan pacifikus ideáját sugározzák, amelyben egy virtuálisan létre-

[18] Manuel Castells: The Network Society: From Knowledge to Policy. In Manuel Castells – Gustavo Cardoso (szerk.): *The Network Society: From Knowledge to Policy.* Washington, Center for Transatlantic Relations, 2005, 20. o.

hozott közösség megvédi csatlakozott tagjait a külső sérelmektől.[19] Ugyanakkor a hontalanná váló világpolgárok a fogyasztói és felhasználó trendek követésével, és a magánéletük sajátos, a biztonság szempontjából indokolatlan megosztásával olyan nyílt társadalmat hozhatnak létre, amely a lokalitás és személyeség hiányában, fizikai segítség nélkül pontosan az egyik meghatározó elemében, a kognitív szférájában a legtámadhatóbb.

Az egyéni aktivitás jelentőségét – az erőszak hagyományos alapdimenzióiban (erő, tér, idő, információ sajátos közegében) – vizsgálva a történelem és a kultúra közösségi kapcsolatainak dinamikus, a természeti és társadalmi törvényszerűségek által kialakuló, vagy a cselekményeket és jelenségeket befolyásolni kényszerülő művi folyamatokként írhatjuk le. Az előzőekben tárgyaltak alapján az egyén aktivitásának megítélése az információs társadalmak technológiai fejlődése során nagyban függ a fejlesztések felhasználásának okától, céljától, módjától és nem utolsósorban hatásaitól. Milyen egyedi biztonságot befolyásoló magatartásformákat fog eredményezni ezen nem állami szintű szereplők beavatkozása, hogyan ítéljük meg a cselekményeket? A kérdést feltehetjük úgy is, mint ahogy azt Farkas teszi 2022 elején az államok védelmi és biztonsági tevékenységével kapcsolatos jogelméleti és kormányzástani kutatásai kapcsán: „az információs technológiák 20. század végi robbanásszerű és azóta is kitartó dinamikával leírható fejlődése az egyénre, a társadalmakra, a gazdaságra, a politikára és értelemszerűen az illegitim/bűnös/szuverenitássértő magatartásokra és az ezek elleni fellépésre nézve vajon hasonló korszakváltást hoznak-e magukkal, mint amilyen a 19–20. század fordulójától a hidegháborúig élt meg az emberiség vagy sem."[20] Az emberiség „új korszaka" sok gondolkodó szerint talán nem is a digitális információs forradalommal kezdődött, hanem inkább annak a multipoláris hatalmi viszonyrendszernek[21] a kialakulásával, amelyben a társadalmi globalizáció katalizátorként működik. Az első fenyegető cselekményekkel 9/11

[19] A közösségi médiában megjelenített versengés meghirdetése nagyon sok követővel számol. Az internet előtti „betelefonálós" műsorokra ugyan már csak az idősebb generációk emlékeznek, de akkoriban is pénzügyi bevételi forrásnak bizonyult egy jól felépített egyszerű kihívás vagy feladvány emeltdíjas telefonszámon történő megoldásának közösségi megosztása. „Az online kihívás (challenge) általában olyan üzenet, felhívás, fénykép vagy videó, amelyben a kihívó valamilyen feladat elvégzésére buzdítja az érdeklődőt. Ez történhet személyesen, szóban, vagy a kihívó akár videóra felvéve is rögzítheti az elvégzendő feladatot, majd valamilyen közösségi portálon közzé teheti, hogy az minél több emberhez eljusson, és minél többen elvégezhessék. Számos fajtája létezik." A nem egy esetben életveszélyes „challenge" végrehajtása, illetve annak megtagadása nemcsak fizikai következményekkel, hanem negatív kognitív hatásokkal is fenyeget. Lásd Csaba Ágnes: Mit érdemes tudni a netes kihívásokról (challenge)? *www.yelon.hu.* 2022. (https://yelon.hu/szuloknek/netes-kihivasok-online-challenge/).

[20] Farkas Ádám: A történelmi tapasztalat és a tudomány helye, szerepe a 21. századi védelmi és biztonsági gondolkodásban. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* 2022/1. szám, 5. o.

[21] Vö. Edward D. Mansfield: Concentration, Polarity, and the Distribution of Power. *International Studies Quarterly,* 1993/1. szám, 105–128. o.

kapcsán szembesült a világ. A terrorcselekményt egy fegyvertelen kis csoport úgy követte el, hogy személyszállító repülőgépeket térítettek el, és szimbolikus jelentőséggel is bíró amerikai épületeket, intézményi központokat vettek célba. A fizikai pusztítás mellett számoltak a kognitív hatásokkal is. A WTC második tornyának összeomlását a – ma élő, aktív – lakosság jelentős része egyenes adásban nézte végig. Fegyverek nélkül sikerült megtámadni az USA-t, és csapást mértek a sebezhetetlen nyugati demokráciák vezető hatalmára. Napokkal később a NATO szövetsége életbe léptette az 5. cikkelyt, amely az egész hierarchikus hatalmi rendszert mozgásba hozta egy államhoz, kormányzathoz, de még egy nemzeti közösséghez, kisebbséghez közvetlenül sem tartozó csoport ellen. A terrorszervezet erejének, hatalmának felszámolását csak hagyományos eszközökkel a földrajzi behatárolás, az afganisztáni műveletek végrehajtása ellenére sem tudták megvalósítani a szövetségesek. A modern emberiség generációit negatívan befolyásoló erőszakkal történő fenyegetések csökkenése, a terror felszámolása egyelőre várat magára, Afganisztánban pedig ismét a nyugati demokráciákkal ellenséges tálibok gyakorolják pusztító hatalmukat.[22]

A kibertér és az ott közvetített fenyegetés legkevésbé sem különös elegye abból az egyéni aktivitásból is levezethető, amely az önmegvalósítás emberi szükséglete mellett a hatalom befolyásolásával kapcsolódik össze. Ahogy arra McLuhan rámutatott, az információtovábbításnak és -megosztásnak létezhet társadalom-, vagyis hatalomformáló szerepe. Ha a 21. század államainak hatalmi területeit és ezen szegmensekre hatással bíró egyéni aktivitását vizsgáljuk, a kibertérben több aktor azonosítható (1. táblázat). A vírustagadó vloggerek és bloggerek írásai és videói éppen úgy negatívan befolyásolták a Covid19 vírus okozta világjárvány kezelését, mint a fenyegetett lakosság biztonságérzetét, az egészségügyi intézmények dolgozóinak tevékenységét, a gyógyszergyártó vállalatok pénzügyi bevételeit, és nem utolsósorban a kormányzatok felelősségi körébe tartozó létfontosságú infrastruktúrák működését, de közvetetten az állami hatalmat is. A közvélekedés szerint bár az etikus hackerek tevékenysége a társadalom tagjai számára hasznosak, mégis a hatalom gazdasági szegmensében felmérhető anyagi és az egyes vállalkozások megszűnésével végződő akciók felmérhetetlen erkölcsi károkat okozhatnak. A hatalom gyakorlásának más területein is megfigyelhettünk kiberaktivistákat[23], akik például a véleménynyilvánítás szabadságára hivatkozva közölnek általuk valósnak értékelt információkat, vagy maguk készített álhírekkel (fake newszal) vagy a mesterséges intelligenciával létrehozott kép- és videóanyagokkal (deepfake-kel) befolyásoljanak egyéni döntéseket, választásokat, vagy toborozzanak fegyvereket, harcosokat, egyszerűen globális híveket fenyegető helyi és regionális konfliktusok, válságok, de még pusztító háborúk

[22] Fencsik Tamás: Éhínség és jogfosztások: a tálib kormány a mélybe taszítja Afganisztánt. *Euronews*, 2022. (https://hu.euronews.com/2022/08/15/ehinseg-es-jogfosztasok-a-talib-kormany-a-melybe-taszitja-afganisztant).

[23] Gémes Csaba: A kibertér és szereplői. *Hadmérnök*, 2018/3. szám, 403–415. o.

támogatására is. Maguk a közösségek által megbízott, felruházott, vagy a közhatalmat gyakorló személyek is tudnak úgy nyilatkozni, hogy a magánvéleményüket és egyéni haszonszerzésüket ne lehessen megkülönböztetni az általuk képviselt közösség elfogadott – nemegyszer pedig kompromisszumok felvállalásával kialakított és deklarált – álláspontjától. Vagy éppen ellenkezőleg, az általuk képviselt közösség álláspontjának tagadásával zavart keltenek, és ezáltal szélesebb elismertséget szereznek maguknak rejtve maradó terveik elősegítéséhez.

1. táblázat. *A kibertérben folytatott egyéni aktivitás lehetséges hatásai a hatalomra (saját szerkesztés)*

A kibertérben folytatott egyéni aktivitás hatása a hatalomra (X)	*A kibertér nem állami szereplői:*[24]		
Az állami hatalom érvényesülésének meghatározó szférái:	*hacker*	*kiberbűnöző*	*hacktivista*
politikai	X		X
gazdasági	X	X	X
szociális	X	X	X
környezeti			X
katonai	X		X

3. AZ INFORMÁCIÓ MINT A FENYEGETÉS ESZKÖZE

A társas énünk az együttélés során kihívásokkal és kockázatokkal néz szembe. Amennyiben ezt bármilyen szinten fenyegetésként éljük meg, az félelmet kelt, és agresszióban, erőszakban csúcsosodhat ki. Leegyszerűsítve – használva a gyakorta emlegetett történelemkönyvek oldalairól visszatükröződő frázist – történelmünk és kultúránk nem más, mint összetűzések és háborúk sora. Jelen korunk bármelyik országa és azok bármilyen szövetsége igyekszik – szuverén módon, legális, közössége által felruházott hatalommal – az alkotó egyének, polgárok (népük, nemzetük, etnikai és egyéb identitásuk) biztonságát szavatolni. A különböző összeütközések, fegyveres konfliktusok nem elszigetelve zajlanak még akkor sem, ha az erő megjelenésének természetéből adódóan jól körülhatárolható földrajzi térhez kötődik.

[24] „A hackerek az informatikai iránt érdeklődő, többnyire a fiatalabb generációkba tartozó személyek, akik informatikai rendszerek, szolgáltatások feltörésével kezdtek foglalkozni, elsősorban a kíváncsiság és a felfedezés öröme által hajtva." – Lásd Gémes: i. m. (2018), 411. o. A kiberbűnözők a számítógéppel követnek el bűncselekmények. Az adott állam törvényei alapján értékelhetők cselekményeik. A hacktivista „a szólásszabadság, az emberi jogok és az információ szabadsága jegyében, számítógépes hálózatokon (általában az interneten) a hackerek által használt eszközöket alkalmazó aktivista". Mozgalmaik „a hagyományos demonstrációk és polgári engedetlenség digitális megfelelői". Lásd Gémes: i. m. (2018), 412. o.

A konfliktusok megelőzéséhez, felszámolásához olyan megoldásokat kell találni, amelyek az információs társadalmak korában a korlátlan infokommunikációs hálózatokban leképezik a földrajzi-fizikai térben megjelenő közvetlen hatásokat, illetve a közvetett hatásokat – az erőkivetítéseket, a valós vagy valótlan híreszteléseket, az emocionális propagandákat – a kognitív térben megjelenő erőszak fizikai kivetülését akadályozzák meg földrajzi környezetünkre. Az információ fegyverré vált.[25]

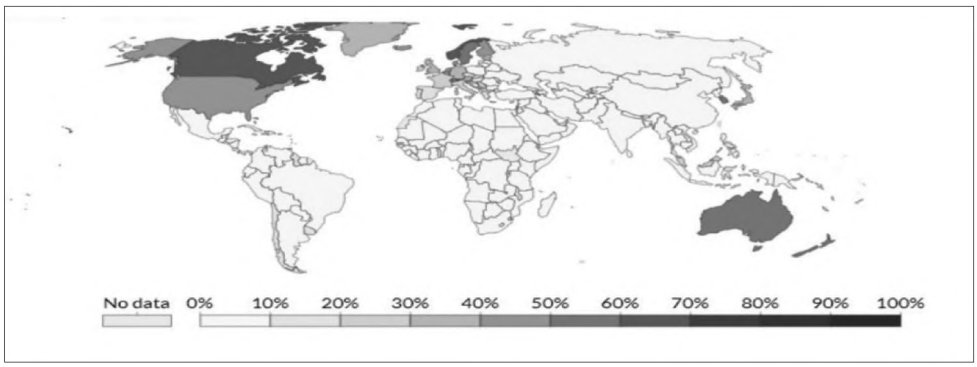
Az életünk jellemző infokommunikációs területein kialakított, illetve önállóan kialakuló egyszerű és bonyolult szerkezeteket, szervezeteket és emberi közösségeket a közvélekedés ugyancsak hálozatokként azonosítja.[26] A csoportokat meghatározó jellemzők egymástól eltérő, egymásra épülő és kijelölt elemeiben kapcsolódásra képes (például politikai, kulturális, szociális vagy ideológiai stb.) rétegeket alkotnak az össztársadalomban. Az egyes szinteken eltérően érzékelhetők a társadalmi folyamatok, események. Belátható és azonosítható időszakokra bontva a csoportok mérete és a hozzájuk kapcsolódó események száma, a hálózatokban megjelenő információ jelentősége növekedést vagy csökkenést, de visszarendeződést és minőségi fejlődést is mutathat. Az idő ebben az értelemben az aktivitás alapdimenziója, hasonlóan a korábbiakban hivatkozott meghatározó hatalmi terekre és az azt fenyegető erőre. A fenyegetés mértékének, illetve az okozott agressziónak az értelmezését több aspektusból, például jogelméleti, hadtudományi, matematikai stb. vizsgálva 9/11 eseménye és az azt követő társadalmi és tudományos diskurzus a kiindulópont.[27]

A 21. század jelentős válságai, valamint következményeik rendre eljutnak kisebb-nagyobb földrajzi tereket érintő fegyveres konfliktusokig. Az orosz–ukrán fegyveres konfliktust több kutatás a 2014-es Euromajdan mozgalomtól vizsgálja, amely jól tükrözi azt a folyamatot, ahogy közösségek hálózatai a közvetlen, illetve a közvetett erőszak mentén összekapcsolódnak, és agresszióval, terrorral párosulva a biztonság elvesztésével járhatnak. Az erőszak és tilalmának megközelítése, a háború és a háborúzás jogának évszázadok óta megújuló egyéni és társadalmi szintű kritikája jelenleg is – többek között a kibertérben zajló események, műveletek, vagy a digitalizációval, mesterséges intelligenciával és felhőalapú információkezeléssel kialakított virtuális terekben, infokommunikációs rendszerekben alkalmazott folyamatok védelmi célú egységesítése kapcsán – folyamatosan zajlik. A kibertér védelme a fizikai és digitális alrendszerek biztonsági fejlesztéseivel növekedett, így egyre több figyelmet kap az információs környezet kognitív szegmensének sérülékenysége.

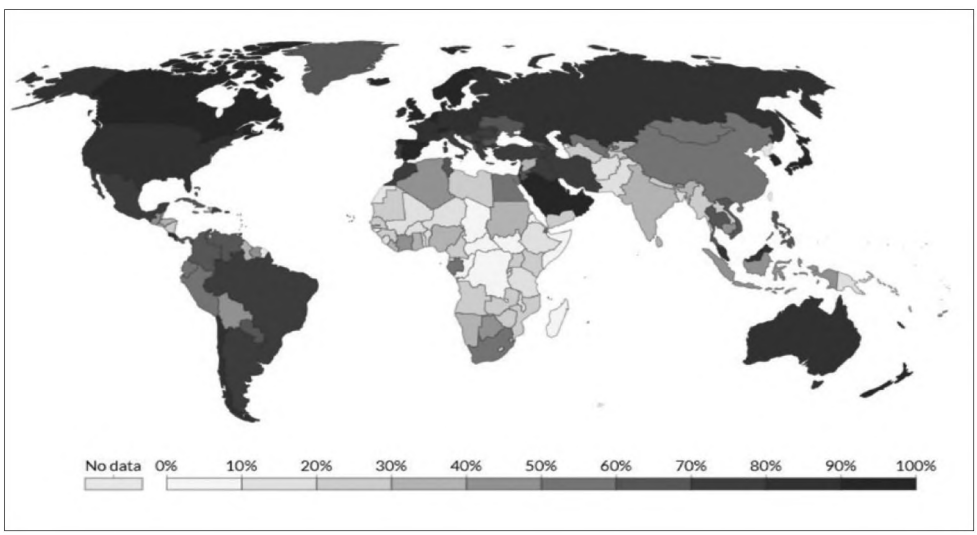
[25] Simon László: A partizán elmélete a premodern virtuális korban: A partizán elmélete az információs környezet speciális műveleteiben. *Jog Állam Politika*, 2017/4. szám, 233–242. o.

[26] A tanulmány keretei nem adnak további lehetőséget arra, hogy a hálozatokkal bővebben, mint a gráfelmélet vagy hálózattudomány tárgyával, vagy a társadalom-lélektan és szerkezetének, a társas kapcsolatok rendszere által meghatározott viselkedésformáknak szociális értelmezésével foglalkozzunk.

[27] Simon: i. m. (2017).

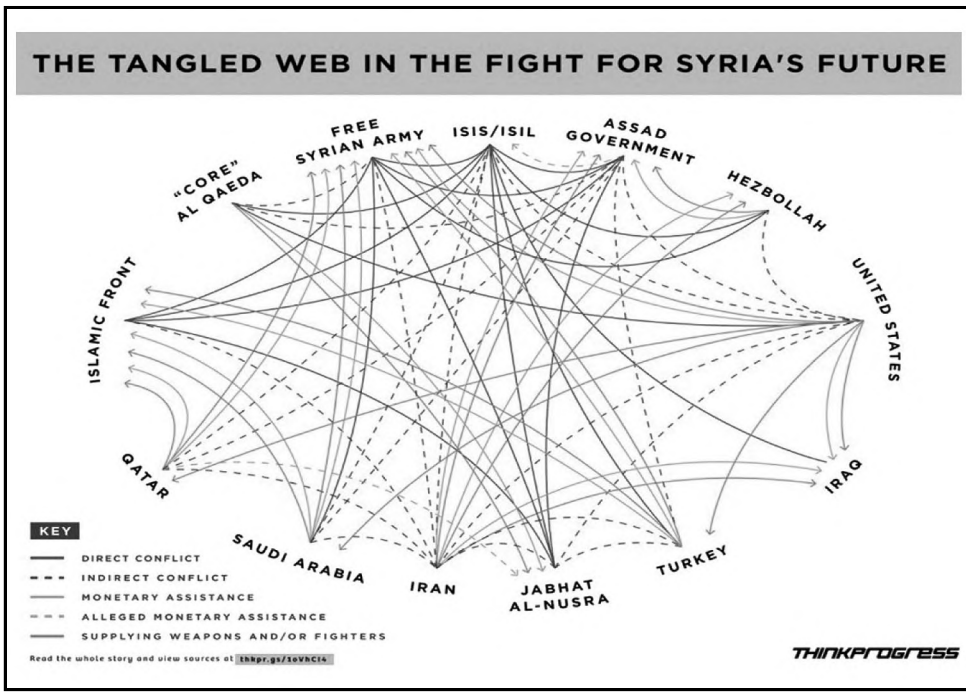


1. ábra. *A világon 2001-ben internetet használók eloszlása országonként (Forrás: Roser – Ritchie – Ortiz-Ospina [2019])*



2. ábra. *A világon 2019-ben internetet használók eloszlása országonként (Forrás: Roser–Ritchie–Ortiz-Ospina [2019])*

A globalizáció során az elmúlt húsz évben a mobil informatikai eszközök és műholdak világméretű elterjedésével (1. és 2. ábra) az egyének, a közösségek, az államok, valamint az NGO-k hatalmi kapcsolatai átalakultak, és kapcsolataik tartalmai is megváltozott. Nemcsak a hatalmat klasszikusan birtokló államok között nem lehet hagyományos a hálózati (multipoláris) hatalmi térben értelmezni a barát és ellenség kétpólusú ellentétpárját, hanem a további hatalmi befolyással bíró szereplők érintettsége miatt sem. Egyre inkább pólusok közötti egyensúly kereséseként kell tekinteni a vitás helyzetek rendezésére. Egyre több résztvevőt kell bevonni a megállapodásba, amely növeli a konfliktus kezelésének és a rendezésnek az időtar-



3. ábra. *Szíria jövőjéért folytatott harcok kapcsolati hálója*
(Forrás: Think Progress [2014])

tamát. Az egységes állami beavatkozás és a szemben álló pólusok egyensúlyának elhúzódó hiánya növeli az érintettek frusztrációit, fenyegetettségét. Az egyéni indíttatású rendezés szükségessége fokozza az önhatalmú beavatkozás, a szélsőséges megnyilvánulások és a radikalizálódás kialakulásának veszélyét. Például a 2011-ben kezdődő szíriai fegyveres konfliktus olyan kapcsolati hálózatot mutatott (3. ábra), amelyben nem alakulhatott ki és a mai napig sem jött létre két pólus. A fegyveres konfliktus intenzitását és az ISIS terrorszervezet fokozatosan növekedő aktivitását és egyéni szintű nemzetközi támogatását ugyan az Oroszországi Föderáció akkori, 2015-ös beavatkozása Bassár Al-Aszad elnök kormányerői mellett (4. ábra) csökkentette. A fegyveres csoportok és a rendezésbe bevonható felek számának 2017-es érdemi csökkenése sem oldotta fel a polarizációt. Hatalmi szempontból pedig a kurd fegyveres csapatok sikerei a konfliktusban csak növelték a térségben regionális szerepüket, így a korábbi török–kurd szembenállás ismét fellángolt. Az orosz–ukrán konfliktus közvetett hatásaként megerősödő Irán szerepe miatt pedig a szíriai válság ebben a régióban 2022-ben is multipoláris megoldást követelne meg.

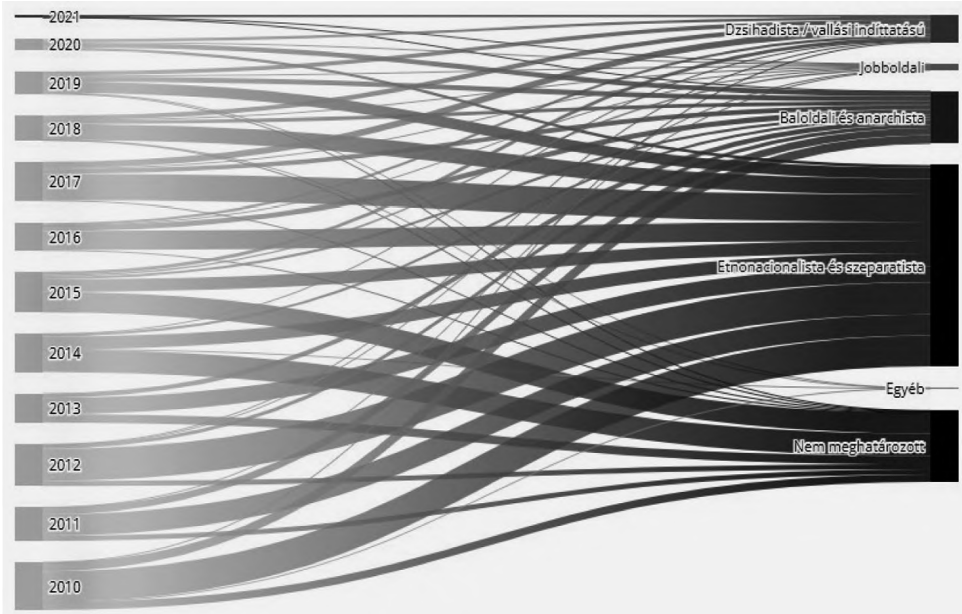
A példa kapcsán rendre a mottóban szereplő uralom hobbesi felfogása mellett a hatalom weberi utalása is szerepet kap, amely szerint a hatalom alapkérdése, hogy miként fogadja el az egyes ember az uralkodó engedelmességének parancsát. A to-



4. ábra. *Az Oroszországi Föderáció szíriai beavatkozásának karikatúrája (Forrás: Latuff [2015])*

vábbiakban visszatérve a multipoláris hatalmi rendszer komplexitása és folyamatos változása okán, a két kultúrájában is eltérő felfogás legitimációs hatását egyszerre kell szem előtt tartani. Ez a legitimáció napjainkban különösen nagy jelentőséggel bír a kibertérben megjelenő fenyegetések esetében, és alapjaiban határozza meg a fenyegetéssel járó verbális agresszió természetét, és az egyéni aktorok, az internetet hatalmi befolyásolásra felhasználók megítélését, válaszlépéseit. Amennyiben elfogadjuk, hogy az államok hatalma az őket alkotó egyének, állampolgárok származtatott többségi akaratából ered, akkor a közösségek szabadsága, továbbá a hatalom „alkalmazott" uralma meg kell jelenjen az egyéni fenyegetések új helyszínén, a kibertérben is.

Mivel a megoldásul szolgáló közös álláspontot nem két, hanem több fél között kellett kialakítani, az információ, a kommunikáció és az együttműködés elengedhetetlenül szükséges a polarizált felek esetében. A 9/11 eseményét követő terrorizmus elleni küzdelem a felelős állami szervezetek (rendőrség, terrorelhárítási és nemzetbiztonsági szolgálatok) országokon átívelő bi- és multilaterális fellépését eredményezte. Ennek egyik alapvető oka az volt, hogy a helyi célpontok azonosításához lokálisan, regionálisan és globálisan rendelkezésre álló információkra volt szükség. Bár korlátozta és nem egy esetben akadályozta az egyes adott államok eltérő jog- és



5. ábra. *Terrortámadások az EU-ban típusonként (2010–2021)*
(Forrás: Europol [2021])

szabályrendszere a válaszcsapások végrehajtását, az információk megosztása létkérdéssé vált. Az egyes terrorcselekményekre adott jogszerű és legitimként feltüntetett válaszok ugyan nem egy esetben a terror spirálját alakították ki.[28]

A közhatalom birtoklásából kiinduló ellentámadás megfelelő egyéni szintű infokommunikációs támogatással, valamint a társadalmak, egyes közösségek meggyőzéséhez elengedhetetlenül szükséges kulturális hatások figyelembevételével párosult. Európában 2010-től fokozódó terrortámadások és terrorcselekmények ellenére a felderítések és a megelőzésre fordított erők 2017-től csökkenteni tudták mind az áldozatok, mind az esetek számát (5. ábra). Az Európát ebben az időszakban jellemző racionális cselekvés, a modern progresszivitás és a fenyegetések reális, azaz a meggyőződésen és a fenntartható kormányzati működésen alapuló hagyományos megközelítése, vagyis a kulturális gyökerű felfogások keveredése jellemezte hol konstruktív, hol pedig destruktív módon.

A 21. századi transznacionális terrorizmus kapcsán átélt események és azok fenyegető hatásai rámutattak, hogy az agressziót az információs társadalmak korában az erő, az idő és tér alapdimenzióján, vagyis fizikai-földrajzi környezetünk mellett

[28] Simon László: A fokozódó terrorizmus Európában és annak hatása a katonai tömegrendezvények biztosítására. *Szakmai Szemle,* 2015/2. szám, 145–162. o.; Simon László – Magyar Sándor: A terrorizmus és indirekt hadviselése az EU kiberterében. *Szakmai Szemle*, 2017/4. szám, 57–68. o.

a kognitív szféránkban is erőszakként éljük meg.[29] A terrorizmus elleni küzdelem tudományos kutatásai rámutattak, hogy bár kódokkal és programokkal nem lehet kioltani életeket, így a kibertérben és annak támogatásával nem lehet klasszikus értelemben fegyveres küzdelmet, háborút folytatni, 9/11 eseményét és az európai terrorcselekmények következményeit közvetett módon, de mindenkinél félelemmel, kiszolgáltatottsággal azonosította. A közvetett és közvetlen műveletekben részt vevő felek különböző minőségű, szintű és intenzitású agressziójában, fegyveres támadásaiban az információ fegyverré vált.

A célpontok minden esetben közvetve vagy közvetlenül mi magunk vagyunk. Az eltérő pólusok mentén közös meggyőződés szerint szerveződő egyének szintjén nem alakulhatnak átfogó elérendő célok. Nem lehetnek kompromisszumok és betartandó elhatározások, mert a pólusokon kialakuló a csoportok között az alkalmi szövetségek és ellentétek folyamatosan változásban maradnak. A szembenállás és kezelésének viszonyrendszere akkor is szerteágazó marad, ha a konfliktus teret kap, legyen az földrajzi vagy attól függő, illetve független virtuális tér. A korábbi korokban megélt fegyveres konfliktusok és szatellitháborúk lovagi küzdelmeknek minősülnek a 21. század fegyveres agresszióihoz mérten. Az információs társadalmak korában a hagyományos tér, idő, erő mellett az eddig támogató funkciót betöltő információ szintén alapdimenzióvá vált. A szemben álló felek pusztító cselekményeinek csökkentésével a konfliktusok kialakulásának megakadályozása, a terror felszámolása és a nyugalom, a béke, a biztonság visszaállítása elérhetetlennek tűnik. A terrorizmusra vagy az aszimmetrikus hadviselésre jellemző politikai hatások, a fegyveres műveletek elkövetésének és eszközrendszerének vitatható átalakulása, továbbá az új hibrid műveletek kialakulása[30] pedig csak növelik az egyének félelmét, és fegyveres vagy egyéb aktivitásukat is.

4. A FEGYVERES KONFLIKTUST TÁMOGATÓ HACKTIVISTA: A KIBERPARTIZÁN

Az orosz–ukrán válság kapcsán napjaink európai népessége is átéli, hogy a terror és erőszak spirálja miatt, a közvetett agresszió elkerüléséhez, annak felszámolásához, a béke kikényszerítéséhez és fenntartásához már a klasszikus értelmű politikai célú akarat kifejeződése, erőkivetítése (például a szankciók bevezetése vagy a NATO-csapatok telepítése Közép-Európába) nem elégséges. Értékelésem szerint

[29] Fekete Csanád: Információ és hadviselés háború a kognitív hadszíntéren II. *Szakmai Szemle*, 2016/3. szám, 24–41. o.; Fekete Csanád: Információ és hadviselés háború a kognitív hadszíntéren II. *Szakmai Szemle*, 2016/4. szám, 46–80. o.

[30] Resperger István: Stratégiák és fogalmak háborúja, az aszimmetrikus hadviselés hadtudományi megközelítése. *Hadtudomány*, 2016/Elektronikus szám.

ennek okaként a jellemzően többpólusú hatalmi hálózatot lehetne megjelölni. Az Oroszországi Föderáció mind az USA-val, az EU-val, mind Kínával, de még alacsonyabb hatalmi státuszú[31] országokkal is politikai, gazdasági és katonai kapcsolatokat alakított ki értékei és érdekei mentén. Nem kívánt, illetve nem tudott korábbi geopolitikai befolyásával élni, nem alakított ki általa vezetett hierarchikus hatalmi rendszert. Ugyanakkor korunk biztonsági kockázatainak kihasználása érdekében modern technológián alapuló képességeket alakítottak ki. Már a szíriai konfliktus esetében is megfigyelhető volt, hogy ha két vagy több fél megegyezik, mindig lesz harmadik vagy korábban „baráti fél", vagy akár egy aktor (például a csecsen származású, georgiai születésű Tarhan Tayumurazovics Batirashvili, azaz Abu Omar al-Sishani), aki közvetett módon, de az információk és az infokommunikációs eszközök felhasználásával – legitim egyéni harcosként – folytatja küzdelmét, toborzó vagy éppen pusztító agitációját.

A világunkban zajló események mögött olyan társadalmi kapcsolatok húzódnak meg, amelyek értékek és érdekek mentén alakítanak ki közösségeket. Ez akkor is igaz, ha a természeti és a mesterséges környezet folyamataira fizikai, biológiai vagy kémiai törvényszerűségeire gondolunk. Az emberi lét kapcsolatai maslow-i és aronsoni értelemben[32] alapvetően határozzák meg eredményességünket is. Az információs társadalmak korában a bipoláris hatalmi rend átrendeződése már nem teszi lehetővé az egysíkú gondolkodást a válságok és konfliktusok értelmezésében. A barát–ellenség fogalompár örök érvényű filozófiai igazsága mára már csak az elmélyült fegyveres konfliktusok legitim és illegitim embertelen terrorjában ismerhető fel. Ahogy Legárd fogalmaz a politika schmitti fogalmából kiindulva: „kizárólag az állam rendelkezik a politika monopóliumával, azaz legitim módon egyedül az állam dönthet arról, ki a barát és ki az ellenség, s hogy az ellenséggel szemben hogyan kell eljárni."[33] Sokkal inkább érvényesül az ellenségem ellensége a barátom filozófia,

[31] Az Oroszországi Föderáció jelenleg nemcsak a legfejletteb nyugati demokráciák által képviselt G8-ban (Group of Eight) vagy az Európai Uniót is magában foglaló G-20-ban, hanem a gazdaság más szegmenseiben is alakított ki tagságokat. Ilyen az OPEC szervezete és a BRIC vagy BRICS közössége, amelyek egyszerre jelentenek a nyugati világtól eltérő regionális és a globális közösséget, továbbá a legfejlettebb országok esetenként kirekesztő közös fellépésével, felfogásával szemben is védettséget, ugyanakkor a nyugati eltérő hatalmi kommunikáció sajátos politikai és gazdasági párbeszéd fórumai. Semmiképpen nem kívánt eltérő kulturális és társadalmi értékei miatt elszigetelt országgá válni. A FÁK, a Kollektív Biztonsági Szerződés Szervezete és az Eurázsiai Gazdasági Közösség pedig azon fórumok, amelyekben dominanciáját fenntartva a legszélesebb fenyegetésekkel is képes szembenézni. Vö. Nagy László – Tömösváry Zsigmond: *Az orosz biztonságpolitikai gondolkodás.* Budapest, Dialóg Campus Kiadó. 2018, 18. o.

[32] A szükséglet és szociálpszichológia két legnagyobb alakja kísérleti úton igazolta, hogy az egyének és azok közösségei miért és milyen motivációval valósíthatják meg önmagukat, illetve milyen jelentősége van a társas megismerésnek a csoportok kialakulásában és egymáshoz való viszonyukhoz.

[33] Legárd Ildikó: A barát és ellenség megkülönböztetése a kibertérben. *Jog Állam Politika,* 2020/3. szám, 137. o.

vagy egy folyamatosan változó összetételű és csak korlátozott együttműködést előrejelző plurális felfogásrendszer.

A részt vevő partnerek vagy szemben álló államok száma – a konfliktusok bonyolultságából adódóan – jelentősen nagyobb lehet, mint kettő. Elhúzódó vagy anómiás válságok esetében a szereplők szövetségesi viszonyrendszere is változékonnyá válhat, de ahogy tapasztaltuk 9/11-et követően, az internet által kijelölt információs környezetben az egyéni aktorok jelentősége megnőtt. Az államok hatalmi képviselete a kibertérben nemcsak azonos elemszámot, vagyis felhasználót mutat a közlések forrását tekintve, hanem a közösségi médiában „követők" nélkül kisebb elismertséget szerezhetnek, mint az influenszerek, azaz a véleményvezérek.[34]

Az emberi viszonyokat alapjaiban meghatározó pszichológiai és szociológiai kötöttségeken túl a döntéseket a felhasználás helye, a vállalt vagy rábízott társadalmi szerep, a kulturális meggyőződés, de még az aktuális fizikai, földrajzi, mentális stb. adottságok is befolyásolják.[35] Ha az információs környezet megszokott lokális megközelítését bővítjük, regionálisan már sokkal árnyaltabban értelmezhetők a fent leírtak. Amennyiben a digitális tartalmakat és a hozzáférhetőségüket tekintjük a fenyegetés fő forrásának, akkor a hacktivisták, habár nem államok, mégis hatalmi-politikai súllyal rendelkezik. Az infokommunikációs hálózatok, így a közösségi média fejlődése növelte az értékelhető internetes tartalmak minőségét és a digitális kapcsolódások számát. A mesterséges intelligencia a prediktív analitikai[36] eljárásai révén érdemi támogatást nyújtanak a hacktivisták ismereteinek elmélyítésében, a tájékozottságuk és egyediségük kifejlesztésében is. A fentiekben leírt 21. századi multipoláris hatalmi rendszer, a meglévő kulturális és gazdasági frusztrációk, de az emberi létünkhöz kapcsolódó önmegvalósítás, vagy akár az azzal összefüggő legitimnek gondolt harc sajátos elegye óhatatlanul megalkotja a hacktivisták azon tagjait, akik egyedül vagy kisebb csoportokban akadályozzák vagy támadják az államok és egyéb nem állami szereplők működését. Bár jogelméleti szempontból ez a fajta fenyegetés is értékelhetővé vált, az internetet átható szabályok rendszere, a felhasználó egyén jogát és kötelezettségét, aktivitásának megítélését, a szankciók rendszerét még nem volt képes minden szegmensben létrehozni. Bár a virtuális térből érkező fenyegetés

[34] Digitalhungary.hu (2021).

[35] Magatartás-tudományi döntéselmélet szerint az egyén általánosan racionálisan hozza meg döntéseit, de rendre a korlátozott racionalitással vagy az inkrementális megközelítéssel élhet. – Kerchner András: *Döntéshozatal. Tréning tananyag.* Miskolc, Miskolci Egyetem Gazdaságtudományi Kar, 2018, 7–8. o. (https://innovativ-tudasvaros-efop361.uni-miskolc.hu/files/1031/Donteshozatal_tananyag.pdf). Lásd még Charles E. Lindblom: *A programalkotási folyamat.* Budapest, Budapesti Közgazdaságtudományi Egyetem – Aula Kft., 1995, 190 o.; James G. March: *Bevezetés a döntéshozatalba.* Budapest, Panem Könyvkiadó, 2000, 296 o.; Simon A. Herbert: *Korlátozott racionalitás.* Budapest, Közgazdasági és Jogi Könyvkiadó, 1982, 311 o.

[36] Szilágyi Szabolcs: Prediktív analitika: a jövőbelátás lehetőségei és korlátjai. *Bitport.hu,* 2015. (https://bitport.hu/prediktiv-analitika-a-jovobelatas-lehetosegei-es-korlatjai-ht-bpc).

és erőszak fizikai értelemben egy kapcsolással, az energia forrásának megszakításával megszüntethető lenne, az agresszió újbóli és újbóli megjelenése az egyes hálózatokban eltérő hatékonysággal ugyan, de esetenként fizikai következményekkel járhat, vagy létfontosságú infokommunikációs létesítmények „információs műveletekkel" történő támadáskor egyenesen életveszélyt is okozhat.[37]

Amennyiben elfogadjuk, hogy közvetett módon egy hacktivista is képes politikai akaratát harcával irreguláris, a kibertér fizikai, információs és kognitív egymásra ható részeiben szervezett módon megvalósítani, akkor a hacktivisták által folytatott kibercselekmények, információs műveletek katonai jellegük és közvetlenül fegyveres konfliktusokhoz való kapcsolatuk alapján elkülöníthető katonai, azaz jogelméleti szempontból más legitim és irreguláris cselekmények katonai értelmezése hasonlóan partizán tevékenységként minősíthető. Az egyén részéről megjelenő, a politikai céljainak eléréséhez vezető információs fölény kialakítása, a kiberfölény kivívása a hacktivistát kiberpartizánná teszi. A 2018-ban lektorált kismonográfiám realista értelmezése szerint[38] „a kibertérben is folytatott küzdelem nem csak a fizikai rendszerek pusztításáról, illetve katonai értelemben az ellenséges célpontok fizikai megsemmisítéséről szól, hanem az állam ellen folytatott politikai célú terrorizmus, illetve partizánharc. A terror és az ellenük folytatott küzdelem jogtudatosságtól távoli indirekt műveleti területe."

***

Félelemmel tölti el a modern demokráciákat az az érzés, miszerint az amerikai és az orosz klasszikus hatalmi központok által korábban determinált világrend a jelenkori biztonságot már nem képesek fenntartani. A nyugati demokráciák által kijelölt hierarchikus hatalmi struktúrákba vetett hite, a béke megőrzésének nagyhatalmi erőfeszítései mellett olyan egyéni szereplők jelentek meg, fenyegetve a lokális és a regionális hatalmi szerepkörök, vagyis egy multipoláris államhatalmi rendszer kiépítését, akik a kibertér és az infokommunikációs hálózatokban megjelenő információk révén irreguláris módon képesek politikai következményekkel járó műveleteket végrehajtani.

A társadalom új közösségi rendszereiben generálisan, így a kibertérben is az egyéni és csoportos szinteken megjelenő ellen- és megerősítő hatások jogi, politikai, szociális és egyéb mélységű párbeszédei, valamint tartalmi együttműködései a jövőnk gyarapodásához, javulásához és biztonságunk növeléséhez kell vezessenek. Ez akkor is igaz, ha az említett hatások – egy adott földrajzi vagy virtuális térben – az eltérő egyéni és közösségi felfogások miatt időben hosszan formálódó politikai, kulturális vagy mentális párbeszéd, illetve az információs befolyásolások okán is

[37] Vö. Simon: i. m. (2017).
[38] Simon: i. m. (2016a).

újabb és újabb konfliktusokhoz vezetnek. Jelen korunk egyéni és magasabb szintű szövetségesi vagy nem állami szintű szereplőinek hatalommal összefüggő vállalásai felértékelik a különböző hálózatokhoz kapcsolódó aktív résztevevőket, erőszakos válaszaik a terror spirálját eredményezik. A katonai és nem katonai értelemben azonosítható cselekvő egyénekkel, aktorokkal, vagy logikai elemekkel (automatikus alkalmazásokkal, mesterséges intelligenciával) szembeni legteljesebb körű fellépés csak úgy csökkentheti félelmeinket, ha a közhatalmat gyakorlók az erőszak állami monopóliumával ebben az új hálózati közegben is képessé válnak az agresszorok azonosítására, cselekményeik illegitim voltát bizonyítani, a megfelelő, jogos és hagyományos értelemben is szankcionálható kibercselekmények köre alakítható ki társadalmi és jogelméleti diskurzus, kommunikáció révén. A fenyegetések esetében felértékelődik az államok szintjén értelmezhető és a kibertérből egyértelműen, projekciók útján levezethető katonai jellegű információs műveletek felderítése, hiszen ezen esetekben mind katonai, mind nemzetbiztonsági reflexiók adhatók.

FARKAS ÁDÁM

A kibertér műveleti tevékenységek egyes szabályozási és államszervezési alapkérdései

A 21. század dinamikus változásainak egyik leginkább érezhető és mindent áthatótó dimenzióját a kibertér és az infokommunikáció fejlődése, életvitelre, társadalmi, politikai, gazdasági működésre gyakorolt hatásai jelölik. Ez a változás pozitív és negatív értelemben is érvényesül. A valós idejű kommunikáció és ezzel a kommunikációra épülő tevékenységek hatásfokának növekedése, vagy épp a személyiség kibontakoztatásának újabb lehetőségei mellett ugyanis a kibertér bűnözésre, befolyásolásra, kémkedésre, illetve hadviselésre is használható, ami jelentős kihívásokat támaszt az államok és társadalmak védelmi funkciói tekintetében. E kihívás fontos jellemzője, hogy egyik oldalról gyökeresen új és változékony technikai sajátosságokkal jellemezhető, másik oldalról pedig a hagyományos működés és életvitel különféle területeit is (át)formálja, ami úgy teszi szükségessé az ezekkel foglalkozó diszciplínák további alkalmazását, hogy közben azok is alkalmazkodjanak az új „dimenzióhoz". Nem véletlen, hogy miközben a kiberbiztonság egy új és önálló területet kezd kialakítani az ernyője alá tartozó ismeretek sokasága és változékonysága miatt, már beszélhetünk a kibertér és internet pszichológiájáról[1], szociológiájáról[2], geopolitikájáról[3] és számos más sajátosságáról is. Mindezek mellett pedig azt is látni kell, hogy a kibertérhez viszonyítva hagyományosnak modható szak- és tudo-

[1] Mary Aiken: *Cyber-csapda – Hogyan változtatja meg az online tér az emberi viselkedést.* Budapest, Harmat – Új Ember Kiadó, 2020; Kiss Tibor – Parti Katalin – Prazsák Gergő: *Cyberdecinacia.* Budapest, Dialóg Campus, 2019; Irene Connolly – Marion Palmer – Hannah Barton – Gráinne Kirwan (ed.): *An Introduction to Cyberpsychology.* London – New York, Routledge, 2016; Caterine Price: *Digitális detox.* Budapest, Libri Könyvkiadó, 2018; Patricia Wallace: *Az internet pszichológiája.* Budapest, Osiris Kiadó, 2002; John R. Suler: *Psychology of the Digital Age: Humans Become Electric.* Cambridge, Cambridge University Press, 2015.

[2] Haim Assa: *Cyberspace and its effect on cultural-political and social processes.* Tel Aviv, Tel Aviv University, 2011.; Desewffy Tibor: *Digitális szociológia.* Budapest, Typotex Kiadó, 2019; Allison Cavanagh: *Sociology in the Age of the Internet.* Maidenhead, McGrawHill Open University Press, 2007; Deborah Lupton: Digital *Sociology.* London – New York, Routledge, 2015.

[3] Amaël Cattaruzza: *A digitális adatok geopolitikája – A hatalom és konfliktusok a big data korában.* Budapest, Pallas Athéné Könyvkiadó, 2020; Farkas Ádám: Biztonság – Geopolitika – Digitalizáció, avagy Amaël Cattaruzza „A digitális adatok geopolitikája" című kötetének főbb üzenetei. *SmartLaw Research Group Working Paper*, 2021/1.; Kieron O'Hara – Wendy Hall: Four Unternets. The Geopolitics of Digital Governance. *CIGI Papers No. 206.* Waterloo, Centre for International Governance Innovation, 2018.

mányterületek nemcsak abban az értelemben vannak megújulási kényszerben, hogy a kibertéri sajátosságokat vizsgálják, hanem abban is, hogy a kibertér hatásait a saját területeikre nézve is elemezzék és alkalmazzák. Ez pedig azt is magától értetődővé teszi, hogy a kibertér biztonságában az újszerű ismeretek és megközelítés mellett a bevett szakmáknak és tudományoknak is komoly – de változó tartalmú – relevanciája van.

Persze látni kell, hogy a témakört még komoly alapkérdések terhelik. Egyik oldalról nem mondható, hogy van egy többségileg elfogadott kibertérfogalom[4], amire építkezhetünk. A fogalmi alapok vitatottsága esetén pedig az arra építkező elvek, eszközök, módszerek, elméletek újragondolása is szükségszerű. Azzal viszont nem tévedhetünk talán túl nagyot, ha a kiberteret egy olyan virtuális, infokommunikációs alapokon álló, de a fizikai valóságtól elkülönülő dimenzióként értelmezzük, amely közvetlen visszahatási képességgel és kapcsolódásokkal rendelkezik a valós, fizikai és mentális életünkre.

Ez a fizikai realitással való kapcsolat és visszahatási potenciál jelentős mértékben képes fokozni a kibertérben rejlő fenyegetések jelentőségét, hatóképességét. Ez pedig értelemszerűvé teszi a kibertérből érkező fenyegetésekkel szembeni védelem szükségességét, illetve a kibertérrel összefüggő biztonság megelőző és reagáló jellegű fokozását. Az államoknak tehát az információs korszakban alapvető működési kötelessége olyan képességek kialakítása, amelyek a kibertérben képesek a katonai, nemzetbiztonsági, illetve rendészeti műveleteket megvalósítani, illetve kooperatív módon a kibertér biztonságos alkalmazásának fenntartásához szükséges működési rendet szavatolni. Ezeket nevezhetjük összefoglalóan kibertérműveleti képességeknek, amelyek kialakításának megkerülhetetlenségét tükrözik azok a tendenciák, amelyek mind a kiberbűnözés elleni fellépés, mind a kibertérben végzett hírszerzés-elhárítás, mind a kibertér és a terrorizmus kapcsolódása, továbbá a kibertérrel összefüggő katonai képességek terén intézményesítési törekvéseket mutatnak a világban.

A transzatlanti térségben fontos alapvetés, hogy ami elválasztja a bűnös magatartásokat a jogszerű vagy engedélyezett cselekményektől, az a jogállamiság követelményéből adódóan a jogi szabályozás általi minősítés, illetve az adott cselekmény megvalósítására való felhatalmazás. Ez az alapelv értelemszerűen a kibertérben vég-

[4] A téma kapcsán lásd például: Michael N. Schmitt (szerk.): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare.* Cambridge, Cambridge University Press, 2017; Michael N. Schmitt (szerk.): *Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge, Cambridge University Press, 2013; Munk Sándor: A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései. *Hadtudomány*, 2018/1. szám, 113–131. o.; Szkála Károly – Munk Sándor: A kibertér fogalma, értelmezése és fejlődése. *Földrajzi Közlemények*, 2018/4. szám, 344–355. o., Kelemen Roland – Németh Richárd: A kibertér fogalmának és jellemzőinek multidiszciplináris megközelítése. In Farkas Ádám (szerk.): *Védelmi alkotmányosság az új típusú biztonsági kihívások erőterében.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2018, 147–170. o.

zett védelmi, biztonsági tevékenységekre is igaz, így jogállami keretek között legalább annyira fontos egy ilyen újszerű, dinamikusan fejlődő terület megfelelő jogi szabályozása és államszervezetben való cizellált leképzése, mint a konkrét képességek fejlesztése, hiszen az utóbbiak a jog megfelelő keretei nélkül nem vagy csak jogellenesen lesznek alkalmazhatók. Nem oktalanság talán arra sem rávilágítni, hogy a szabályozottság egyben rendszerezettséget is feltételez, ami globális értelemben – a jogállami kereteken kívül – is nélkülözhetetlen, hiszen a kibertér lényegében infokommunikációs rendszerek hatalmas decentralizált hálózata, ami olyannyira sokrétű és kiterjedt, hogy szabályozottság természetéből adódó sematizálást nem tudja nélkülözni.

A jogi szabályozottság követelményére tekintettel megkerülhetetlen, hogy a kibertérben végzett tevékenységek jogi keretei újszerűek legyenek. Ehhez a szakmai és jogi követelmények szinkronizálása, a szakemberek együttműködése és együttgondolkodása alapfeltétel. Önmagában a kibertérhez kapcsolódó – műszaki – tudományok és szakmák nem tudják jogállami keretek között megoldani a kibertér áldásai mellett megjelenő fenyegetések kezelését, míg a szakmai támogatás nélkül a jogalkotó sem tudja kezelni az előtte álló kihívást. Fontos azonban e téren látni, hogy amiképp a kibertér nem egy szeparált, kizárólag virtuális, azaz a valós élettől és annak területeitől külön létező valóság, hanem egy olyan újszerű síkja a létezésnek, ami lényegében minden tevékenységre képes jelentős mértékben ráhatni, úgy a szabályozás sem lehet kizárólag elkülönülő jellegű, vagyis a kibertér viszonyait önállóan, minden mástól elválasztó módon rendező. A kibertérben végzett tevékenységek szabályozásának a sajátos törvényi keretek mellett meg kell jelennie a védelem klasszikus szabályrendszereiben és jogszabályaiban is, sőt minden olyan kapcsolódó terület és viszonyrendszer szabályozásában és fogalomrendszerében, amelyre a digitalizáció érdemi hatást gyakorol, és ezáltal tartalmában módosít.[5] Ezt jól példázzák mindazok a területek, amelyek már reagáltak a digitális tartalomközlésre, illetve a digitális térben végzett cselekményekre a hírközléstől, a szellemi alkotások jogán át a büntetőjogig.[6] E területek kapcsán pedig látni kell, hogy ezeknek is van a komp-

[5] Ennek egyik példáját adhatják az emberi jogokkal kapcsolatos háttértanulmányok, illetve Kelemen Roland gondolatai az alapvető jogok és a derogáció vonatkozásában. Vö. AHRC: *Background paper: Human rights in cyberspace.* Sydney, Australian Human Rights Commission, 2013; Kelemen Roland: A derogáció értelmezése a Polgári Jogok Nemzetközi Egyezségokmányának, valamint az Emberi Jogok Európai Egyezményének tükrében. *Közjogi Szemle*, 2018/4. szám, 52–58. o.

[6] Példaként lásd Harkai István: Végfelhasználói jogok a digitális szerzői jogban: Felhasználói jogok…? In Strihó Krisztina – Szegedi László (szerk.): *Európai szabályozáspolitikai kihívások.* Budapest, Ludovika Egyetemi Kiadó, 2022, 25–31. o.; Eck Gábor: Az online terrorista tartalmak elleni fellépést támogató uniós és magyarországi intézkedések. *Külügyi Műhely,* 2022/4. szám, 34–48. o.; Timár Adrienn: Digitális szerzői jog. In Sajtiné Sándor Erika (szerk.): *Bevezetés a szerzői jogba.* Budapest, Szellemi Tulajdon Nemzeti Hivatala, 2020, 40–44. o.; Ződi Zsolt: Az európai platformszabályozás jellegzetességei. *In Medias Res* 2022/1. szám, 66–82. o.; Török Bernát – Ződi Zsolt (szerk.): *Az internetes platformok kora.* Budapest, Ludovika Egyetemi Kiadó, 2022; Bartkó Róbert – Gál István László: A kibertérben

lex biztonság horizontjához való közvetlen kapcsolódása, hiszen egyértelműen hatnak a törvényes rend érvényesülése mellett a társadalmi és gazdasági működésre, végső soron pedig a stabilitásra.

Az önálló és emellett főként a védelem már meglévő jogi kereteibe beépülő szabályozás meglátásom szerint csak úgy valósítható meg, ha a kibertérben végzett tevékenységeket nagyrészt sikerül koherens módon elhelyezni a nemzetközi és a nemzeti jog szöveteiben. Ez egyrészről nemzetközi összehasonlító elemzést, másrészről komplex stratégiai szemléletet, harmadrészről pedig a nemzeti szabályozásunk széles látókörű megújítására való nyitottságot feltételez. Ezek és különösen az ezekhez szükséges szakemberek, tudományos kutatók és komplex tudományos kutatások tehát a megfelelő jogi és működési keretek kialakításának zálogai. Jelen tanulmány a fegyveres védelemmel összefüggő komplex és más újszerű területekre és jelenségekre reagáló kutatások élénkülésére[7] is tekintettel e kérdések egyes aspektusaira tér ki.

1. A SZAKMAI KÖVETELMÉNYEK, A NEMZETKÖZI JOG ÉS A NEMZETÁLLAMI SZABÁLYOZÁS HÁROMSZÖGÉBEN

A kibertérműveleti képességek fejlesztése és szabályozása tekintetében fontos rögzíteni, hogy több szempontból is adódik a komplex és multidiszciplináris megközelítés megkerülhetetlensége és vele az egyes – szakmai vagy épp ágazati – szereplők kizárólagosságának értelmezhetetlensége. A *szakmai dimenzió* tekintetében fontos ugyanis kiemelni, hogy nemcsak a szűken értelmezett kibervédelmi és -biztonsági funkciókat ellátó szakterületekre, hanem a tágabb IT-szakterületre, sőt még az ehhez kapcsolódó szakterületekre – szervezés, jog, műszaki támogatás, stb. – is fokozott figyelmet kell fordítani, idekapcsolva az innováció kérdéseit és nemzeti szintű szervezését is. Ezt erősíti az a fenti érvelés is, hogy a valóságra való visszahatási képesség miatt a „hagyományos" diszciplínák bevonása és egyben fejlődése is adekvát. Szintén figyelembe veendő, hogy a multidiszciplináris tudományos megközelítés mellett a vállalatvezetési kultúrában is erősödő specialisták-generalisták kérdés-

megjelenő büntetőjogi kihívások és fenyegetések kezelésének tendenciái. *Military and Intelligence CyberSecurity Research Paper,* 2022/12.; Mezei Kitti: Új tendenciák a kiberbűnözés büntetőjogi megítélésében. In Gárdos Orosz Fruzsina (szerk.): *A magyar jogrendszer rezilienciája 2010–2020,* Budapest, ORAC Kiadó Kft., 2022, 529–549. o.; Mezei Kitti: *A kiberbűnözés aktuális kihívásai a büntetőjogban.* Budapest, L'Harmattan Kiadó – MTA Társadalomtudományi Kutatóközpont, Jogtudományi Intézet, 2022.

[7] E tekintetben példaként lásd Spitzer Jenő: *Önvédelem versus terrorizmus. Az erőszak tilalma és az önvédelem joga a nemzetközi jogban, különös tekintettel az Iszlám Állam elleni nemzetközi fellépés lehetőségeire.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2019; Farkas Ádám (szerk.): *Védelmi alkotmányosság az új típusú biztonsági kihívások erőterében.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2018; Farkas Ádám: *A fegyveres védelem mint állami alrendszer és annak szabályozási sajátosságai.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2018.

kör is transzformálható erre a területre.[8] Nyilván az egyes szakmai rétegeknek vagy szegmenseknek nem lehet azonos a súlyozása akkor, amikor kifejezetten kibertérműveleti képességek kialakításáról van szó, másik oldalról viszont a biztonsági és védelmi karakter súlyozása nem eredményezheti a kapcsolódó szakmai kritériumok súlytalanodását sem. Ez utóbbi ugyanis az esetlegesen elért eredmények és fejlesztések támadhatóságát is növelheti, például akkor, ha a nem megfelelő jogi keretek miatt az alkalmazó-fejlesztő állam jól strukturált ellenlépések célkeresztjébe kerül.[9] Ez mind a szakmai-kidolgozói, mind pedig a kormányzati, irányítói, illetve szabályozói szintű teendők szempontjából fontos alapvetés, ami a fejlesztendő képességekkel érintett tér, azaz a kibertér sajátosságaiból éppúgy következik, mint a biztonság komplexitásából.

Egyrészről a kibertér azon jellemzője, hogy az a valóságnak egy fizikai kötődésekkel rendelkező és a fizikai valóságba visszahatni képes, de nagyrészt virtuális része, egyértelművé teszi, hogy a hatásait a védelem terén a 20. századig megszokott külső/belső védelmi funkciófelosztástól függetlenül, átfogó jelleggel fejti ki. Ez meglátásom szerint a legtöbb új típusú kihívás, illetve a hadviselés változásai folytán általánosan jellemző a védelem terén.[10] Ezért úgy is fogalmazhatnék, hogy a kiber-

[8] A téma kapcsán lásd David Epstein: *Sokoldalúság.* Budapest, HVG Könyvek Kiadó, 2021; Steven Koetler: *A lehetetlen művészete.* Budapest, HVG Könyvek Kiadó, 2021.

[9] E lehetőségek egyikét tükrözi a lawfare, a joggal való hadviselés opciója, amely egyik variánsában a hibás vagy hiányos nemzeti/nemzetközi szabályozás kiaknázásával törekszik delegitimálni és diszkreditálni a megcélzott államot, amelyre így gazdasági, diplomáciai, belpolitikai hatások hárulhatnak. A téma kapcsán lásd Charles J. Dunlap Jr.: *Law and Military Interventions: Preserving Humanitarian Values in 21 st Conflicts.* (https://people.duke.edu/~pfeaver/dunlap.pdf); Sascha Dov Bachmann – Andres B. Munoz Mosquera: Lawfare and hybrid warfare – how Russia is using the law as a weapon. Amicus Curiae. *Journal of the Society for Advanced Legal Studies*, Summer 2015, 25–28. o.; Tawia Ansah: Lawfare: A Rhetorical Analysis. *Case Western Reserve Journal of International Law*, 2010, 87–119. o.; Hódos László: A hibrid konfliktusok felívelési szakasza, avagy a fenyegetés észlelésének, megelőzésének és kezelésének nemzetbiztonsági aspektusai. *Honvédségi Szemle*, 2020/4. szám, 49–64. o.; Petruska Ferenc: A lawfare tipológiája. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok*, 2022/16. szám; Petruska Ferenc: Lawfare a védelmi szférában. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok*, 2022/18. szám; Petruska Ferenc: A jogi hadviselés eszköztára. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok*, 2022/17. szám; Petruska Ferenc: A Lawfare fogalma. *Katonai Jogi és Hadijogi Szemle*, 2021/3. szám, 97–106. o.

[10] Az átfogó jelleg és ezzel szemben a reziliencia fejlesztése a NATO-ban is alapvetés ma már. Ezt a hatást a nemzetközi terrorizmus, a hibrid konfliktusok és ezekhez kapcsolódva vagy épp önállóan a kibertérből érkező fenyegetések, támadások váltották ki. Azt is mondhatnánk, hogy a 21. század meghatározónak és újszerűnek tartott biztonsági fenyegetései komplexek, differenciáltak, a védelem szempontjából ágazatokon átívelők, azaz totálisak. A totális biztonsági kihívások, a hibrid konfliktusok alapjellemzője, illetve a nemzetközi terrorizmus kapcsán lásd Gregory F. Treverton – Andrew Thyedt – Alicia R. Chen– Kathy Lee – Madeline McCue: *Adressing Hybrid Threats.* Stockholm, Swedish Defence University, 2018; Tiina Ferm: *Laws in the Era of Hybrid Threats.* Helsinki, The European Centre of Excellence for Countering Hybrid Threats, 2017; Christopher S. Chivvis: *Understanding Russian "Hybrid*

térből érkező fenyegetések tekintetében a külső/belső védelmi felosztás éles elhatárolása nem értelmezhető, hiszen a decentralizáltan globális hálózati jelleg kizárja a nemzetállami határok mentén történő leválasztásokat a legtöbb esetben. Ebből adódóan tehát egyik oldalról az érintett ágazatoknak, illetve katonai karakterű szervezeteknek[11] képesnek kell lennie a saját maguk tekintetében szükséges, speciális kibertérműveleti és védelmi feladatok ellátására, emellett viszont a fokozott együttműködésre is. Hasonlóan fontos a kooperáció tekintetében az, hogy a kiberbiztonság fenntartásához a tervezés és felkészítés szintjén is szinkronizálni kell a különféle védelmi-biztonsági szférákat a „civil" társadalommal, sőt okszerű a határokon átívelő együttműködések erősítése is.

Másrészről maga a kibertér is egy hatalmas és rendkívül összetett hálózat. Az onnan érkező fenyegetések is hálózatos jellegűek, aminek az is fontos következménye, hogy a kibertérben való közvetítésen túl ezek mind módszerük, mind célpontjaik, mind hatásterületük és hatásaik tekintetében differenciálódhatnak. Ennek megfelelően a kibertérből érkező fenyegetésekkel szembeni fellépésnek is differenciáltnak és hálózatosnak kell lennie. Azaz a kibertérműveleti képességeknek – az interoperabilitásra való alkalmassággal – meg kell jelennie a klasszikus rendészeti, katonai, nemzetbiztonsági feladatokat ellátó szervezeteken és a tág értelemben vett civil-állami együttműködés keretein és architektúráin belül, illetve akár az egyes ágazatok vonatkozásában új, önálló szervezeti keretekben is. Ez a fajta, a fegyveres védelem rendszerének egészét érintő megjelenés vagy leképeződés azonban szintén a multidiszciplináris szemlélet felé mutat, hiszen az egyes védelmi ágazatoknak és szervezeteknek eltérő igényei, céljai, eszközei, eljárásai és szervezeti keretei lesznek. Ez a fajta fejlesztés tehát az ágazatok vonatkozásában hasonló ívet kell, hogy bejárjon, mint a nemzetbiztonsági szolgálatok fejlődése a 20. században, ami az önállóvá válás

---

Warfare" and What Can Be Done About it. Santa Monica, RAND Corporation, 2017; Michael Weiss – Hassan Hassan: *Az iszlám állam.* Budapest, HVG Könyvek, 2015; Rainer Hermann: *Az iszlám állam.* Budapest, Akadémiai Kiadó, 2015; Loretta Napoleoni: *Az iszlamista főnix.* Budapest, HVG Könyvek, 2015; Farkas Ádám: *A totalitás kora? A 21. század biztonsági környezetének és kihívásainak totalitása és a totális védelem gondolatkísérlete.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2018.

[11] Kutatásim során egyik fő munkafogalmam a katonai karakterű szervek fogalma. Katonai karakterű szerveken a legitim, szabályozott, monopolizált és szervezett állami erőszak érvényesítésére törvényileg feljogosított, – főszabály szerint – katonai rendfokozati hierarchiában, parancsuralmi vezetési rendszerben és a szervezet egészét általánosságban jellemző fegyveres jellegben működő testületeket értem. Ez a kategorizálás ebben a formában nem tesz különbséget sem aszerint, hogy az adott szervezet fő funkciója belső vagy külső védelmi, sem aszerint, hogy mely védelmi ágazathoz tartozik a szervezet, sem pedig aszerint, hogy a szervezet beleérthető-e valamelyik már használt, bevett – de nemritkán vitákkal terhelt – fogalmi körbe, mint amilyen a fegyveres erő, a rendészeti szervek, rendvédelmi szervek vagy a nemzetbiztonsági szolgálatok. Fontos azonban kiemelni, hogy ez egy rendszerező, tehát tudományos, elméleti fogalom, és nem egy alternatíva a katonai, nemzetbiztonsági, illetve rendészeti szervek legális fuzionálására.

mellett a meglévő védelmi funkciókat támogató jelleggel, azokhoz igazodó – polgári-katonai – differenciálódással épült ki a világ számos pontján.[12]

A differenciált és hálózatos szakmai igények és megoldások mellett, illetve ahhoz szorosan kapcsolódó módon a nemzetállami és a nemzetközi jogi vonatkozásokban is komolyan egymásra ható erőterek fedezhetők fel. Ezekhez a kibertérműveleti képességek fejlesztésének alkalmazkodnia kell. Ez a tagolás azonban nem értelmezhető a szakmai/ágazati tagoltságtól függetlenül, hiszen magától értetődő, hogy mind a nemzeti, mind a nemzetközi jog terén rendkívül eltérő szabályozási anyag vonatkozik például a rendészeti, a katonai, a nemzetbiztonsági, illetve a különféle szakigazgatási funkciók ellátására. Ez a jogi értelemben vett sokrétűség azonban a kibertérműveleti képességek kiaknázása, illetve az azokkal kapcsolatos garanciák terén komoly jelentőséget nyer.

A *nemzetközi jogi vonatkozások* terén ugyanis látható az a tendencia, hogy a *katonai funkciók* tekintetében van egy meglehetősen erőteljes és kiforrott szabályozás, mind a korlátozások, mind a lehetőségek, mind a cselekmények értékelése tekintetében. Ennek megfelelően a katonai kibertérműveleti erők a nemzetközi jog vonatkozásában osztják a katonai erők sorsát és szabályozását. Ezt a témát mindenképp fontos Magyarországon is részletekbe menően elemezni, azt azonban a jelen áttekintés szintjén sem lehet elmulasztani, hogy a NATO szintjén is nyitott kérdésre hívjuk fel a figyelmet a kibertéri (nem kinetikus) és a kinetikus műveletek és hatások relációja terén.[13] Nem véletlen, hogy a NATO hadszíntérré nyilvánította a kibertéret, és a nemzetközi jog vonatkozó szabályait alapvetően alkalmazhatónak tekinti az ott folyó katonai műveletekre is.[14] Érdekesebb kérdés persze, hogy a nemzetközi jog által kevéssé kiforrottan kezelt hírszerzés égisze alatt megvalósuló kibertéri műveletek sorsa miként alakul, illetve hogy például a nemzetközi bűnügyi együttmű-

[12] A téma kapcsán lásd Christopher Andrew: *Titkos világ I–II.* Budapest, Európa Könyvkiadó, 2021; Farkas Ádám: Gondolatok a nemzetbiztonság fogalmáról. *Szakmai Szemle,* 2020/3. szám, 5–20. o.

[13] A kinetikus hatások és válaszok kérdései kapcsán lásd például Scott D. Applegate: The Dawn of Kinetic Cyber. In K. Podins – J. Stinissen – M. Maybaum (szerk.): *2013 5th International Conference on Cyber Conflict Proceedings.* Tallinn, NATO CCD COE Publications, 2013, 163–177. o.; Kenneth Geers (szerk.): *Cyber War in Perspective: Russian Aggression against Ukraine.* Tallinn, NATO Cooperative Cyber Defence Centre of Excellence, 2015; David Wallace: Cyber Weapon Reviews under International Humanitarian Law: *A Critical Analysis. Tallinn Paper No 11.* Tallinn, NATO Cooperative Cyber Defence Centre of Excellence, 2018; Kelemen Roland – Pataki Márta: A kibertámadások nemzetközi jogi értékelése. *Katonai Jogi és Hadijogi Szemle,* 2015/1. szám, 53–90. o.; Lattmann Tamás: Nemzetközi jogi szabályozás célzott kibertámadások esetén. Deák Veronika (szerk.): *Célzott kibertámadások.* Budapest, Nemzeti Közszolgálati Egyetem, 2018, 39–51. o.; Alexander Klimburg (szerk.): *National Cyber Security Framework Manual.* Tallinn, NATO Cooperative Cyber Defence Centre of Excellence, 2012.

[14] E tekintetben lásd Csiki Tamás – Tálas Péter – Varga Gergely: A NATO walesi csúcstalálkozójának napirendje és értékelése. *Nemzet és Biztonság,* 2014/4. szám, 112–128. o.; NATO: Wales Summit Declaration (https://www.nato.int/cps/ic/natohq/official_texts_112964.htm); Tálas Péter: A varsói NATO-csúcs legfontosabb döntéseiről. *Nemzet és Biztonság,* 2016/2. szám 97–101. o.; NATO: Warsaw Summit Communiqué (https://www.nato.int/cps/en/natohq/official_texts_133169.htm).

ködés kibertéri hatékonysága miként értékelhető. A katonai dimenzióban közkeletű kérdés, hogy egy jelentős kibertérműveleti csapásra az önvédelem keretében – az arányosság fokmérőihez igazodva – akár kinetikus választ is lehet-e adni, és hol húzódik ennek a határa. A katonai kibertérműveleti erők szabályozása, alkalmazása, illetve ezekhez igazodó felépítése terén tehát a nemzetközi jogi szabályozásra és korlátozásra a politikai, diplomáciai, gazdasági, illetve adott esetben egy fegyveres konfliktusból eredő hatások miatt fokozott figyelmet kell fordítani. E figyelem fókuszán pedig nem kerülhetnek kívülre más modern hadviselésre – is – alkalmazott eszközök nemzetközi jogi tapasztalatai, akár a drónok, akár az autonóm fegyverrendszerek viszonylatában. Feltehető ugyanis, hogy az ott már államok által bejárt utak – például a mozgástér bővítésére – a kibertér kapcsán is érvényesülni fognak, akárcsak azok a megoldások, amelyek a katonai-hírszerzési-bűnüldözési képességek kombinálásával lényegében osztott jogi alapokat generálnak.[15] Ez a még formálódó, mégis több tekintetben már beazonosítható elemekkel bíró nemzetközi jogi keretrendszer értelemszerűen determinálja a nemzeti szintű szabályozást is, mintegy korlátozva azt a geopolitikai realitás körülményeivel.

Hasonlóan korlátos azonban *a rendészetre* vonatkozó nemzetközi szabályrendszer is, hiszen azt a nemzetközi jog a szuverenitás klasszikus belső megnyilvánulásaként fogja fel. A határokon átívelő fenyegetésekkel kapcsolatos bűnügyi egyezmények közül persze kiemelhető itt a Budapesti Konvenció[16], fontos azonban azt rögzíteni, hogy sem ez, sem más bűnügyi egyezmények alapvetően nem írják felül azt a tényt, hogy a rendészet alapvetően a szuverenitás belső funkcióihoz tartozik. A rendészeti kibertérműveleti erők mozgástere tehát – főszabály szerint – a nemzetállamon belül, a nemzeti eljárások vonatkozásában értelmezhető. Azon túl csak kifejezett, szabályozott és határozottan erre is kiterjedő nemzetközi bűnügyi, rendészeti együttműködés keretében valósulhat meg a rendészeti fellépés, vagyis a szuverenitás belső szegmensének a külsőbe való átmozdulása. E tekintetben azt is ki kell emelni, hogy bár a fegyveres erő alkalmazása és fegyveres támadás kapcsán joggal asszociálunk klasszikusan katonai cselekményekre, azonban a kibertérben megvalósuló ilyen cselekmények kapcsán elsődlegesen az adott államnak való betudhatóság dominál (attribúció). Ennek megfelelően a határon kívülre irányuló, egy állam rendészeti kibertérműveleti képességével végrehajtott támadó jellegű műveletek kapcsán felmerülhet a fegyveres erőalkalmazásnak minősítés kérdése a sértett állam részéről, függetlenül attól, hogy azt pro forma nem katonai szervezet hajtotta végre. A kifelé irányuló cselekményeknél ugyanis az államnak való betudhatóság és a cselekmény hatásai jelentős mértékben határozzák meg a minősítést, ami mellett a nemzetállamon belüli szervezeti kategorizálás másodlagossá válik. Erre figyelemmel alakul

[15] Példaként lásd Farkas Ádám: The UK'S National Cyber Force – Beginning of a Hybrid Trend or a New Answer for Cyber Domain. *Military and Intelligence CyberSecurity Research Paper,* 2022/2.

[16] Budapest Convention on Cybercrime (ETS No. 185), Budapest, 23/11/2001.

ki az a jellemző megoldás a transzatlanti térségben, hogy a kifejezetten támadó képességek a nemzetközi és nemzeti jog korábbi korlátozó szabályrendszereihez jól igazodó fegyveres erőkhöz kerülnek telepítésre, míg a rendészeti szerveknél alapvetően a bűnfelderítést támogató, a rendészeti rendszerek védelmét szolgáló, illetve az esetleges nemzetközi bűnügyi együttműködésben is alkalmazható képességek kialakítása valósul meg. Persze a nemzetállami érdekek érvényesítése a két „véglet" közötti mozgásteret is szükségessé tehet, ami a jellegéből adódóan titkossággal párosuló nemzetbiztonsági/hírszerzési/titkosszolgálati tevékenységekben ölthet testet.

A nemzetközi jogi szabályozás terén *a nemzetbiztonsági, pontosabban a hírszerző és elhárító funkciók* vonatkozásában találkozunk a legalacsonyabb szintű, tehát egyik oldalról bizonytalanságot okozó, másik oldalról a rugalmasságot lehetővé tevő szabályozással. A kibertérben végzett hírszerzés és elhárítás is osztja a klasszikus hírszerző – kémkedő –, illetve elhárító tevékenységek sorsát a nemzetközi jog tekintetében. E körben – szemben a katonai fellépésre, vagy épp a más ország szuverenitását sértő módon túlterjeszkedő rendészeti fellépésre vonatkozó szabályokkal – kiforrott és részletes nemzetközi jogi szabályrendszerről nem beszélhetünk. A fő rendező elv az, hogy a kémkedéssel szemben a nemzetállam jogosult jogi eszközökkel fellépni, míg kimunkált nemzetközi jogi rendszer emögött érdemben nem áll. Ez persze nem zárja ki, hogy egy nagy hatású, kibertérben végrehajtott nemzetbiztonsági művelet ne lehetne utóbb a szuverenitást jelentősen megsértőnek értékelhető a megcélzott állam által, de az e szint alatti cselekményeknél általában a hangsúly a nemzetállam védekezésén, illetve a nem jogi következményeken van. Egy kiberhírszerző[17] (adott esetben hibrid hadviselésbe illeszkedő, de még nem nagy intenzitású befolyásoló) művelet a dekonspiráció esetén is csak további feltételekkel valósíthat meg erőalkalmazást. Ez azonban egyértelműen nem eredményezi az ellenérdekelt fél önvédelmi helyzetbe kerülését. E tekintetben külön kérdéses és vizsgálandó, hogy a betudhatóság megáll-e az adott – sokszor áttétekkel, nem állami szereplők felhasználásával megvalósuló – cselekmények vonatkozásában. Erre nézve vannak ugyan az egyes államoknak rugalmasabb értelmezési lehetőségei, de azt a nemzetközi bírói gyakorlat törekszik keretek közé terelni. A jogi minősítés persze sem a hírszerzési, sem a diplomáciai, sem a gazdasági válaszokat – a realitásban – nem zárja ki. Ennek köszönhető az, hogy számos NATO-tagállam a kibertérműveleti képességeit mind a polgári, mind pedig a katonai oldalon beágyazza a nemzetbiztonsági szolgálatok feladatrendszerébe, hiszen azokra nézve elsősorban a nemzeti jogszabályi környezet irányadó, míg a nemzetközi jog terén egy rugalmasabb, bizonytalanabb keretrendszer ragadható meg csak.

[17] A téma kapcsán példaként lásd Katharina Ziolkowski: Peacetime Cyber Espionage – New Tendenciesin Public International Law. In Katharina Ziolkowski (szerk.): *Peacetime Regime for State Activitiesin Cyberspace International Law, International Relations and Diplomacy.* Tallinn, NATO Cooperative Cyber Defence Centre of Excellence Publication, 2013, 425–464. o.

A nemzetközi jogi keretekre figyelemmel *a nemzetállami jogi szabályozás*ra mint a kibertérműveleti erők fejlesztését és alkalmazását determináló erőtérre kell kitekintenünk. Ebben az erőtérben a különféle államon belüli és államokon átívelő szakmai erőhatások, a nemzetközi jogi és a geopolitikai erők, továbbá a képességek – innovációs és gazdasági – korlátossága egyaránt találkozik. Egyrészről ugyanis nyilvánvaló, hogy az adott állam fegyveres védelmi rendszerén belül az ágazati tagozódás, a szervezeti mátrix és az ehhez kapcsolódó hatáskör- és képességmegosztás, valamint az ezeket irányító kormányzati felelősségi és döntéshozatali szisztéma is a nemzeti jog és politika által meghatározott. Ez a nemzetállami jogi szabályozás szükségképpen tükrözi az adott állam kulturális, történeti, geopolitikai és geostratégiai helyzetét és sajátosságait, ami mellett fontos azt is hangsúlyozni, hogy a nemzeti jogrendszer határozza meg az adott állam védelmi képességeinek és eljárásainak alapvető és elsődleges szabályait, méghozzá az adott állam politikai döntéshozóinak a preferenciái szerint. A nemzetállami szabályozás tehát az adott állam szakmai és nemzeti tradícióihoz és történeti tapasztalataihoz nagyban igazodó módon rendezi a védelmi funkciók, vagyis ennek részeként a kibertérműveleti erők szabályozását is, de úgy, hogy a nemzeti keretrendszerbe a politikai mérlegelés függvényében kerülnek be a szakmai és a nemzetközi jogi elemek. Ezen sajátosságok jelentőségét tükrözi, hogy Georg Nolte – a német védelmi minisztérium megbízásából – már a kétezres évek elején összehasonlító elemzés tárgyává tette az európai katonai jogi rendszereket,[18] és ennek részeként osztályozta az európai államok szabályozását. Ez az elemzés markáns eltéréseket mutatott ki az egyes államok szemléletében és szabályozásában, ami mind a NATO, mind az EU védelmi harmonizáció vagy integráció tekintetében kulcsjelentőségű. E vonatkozásban azt is hangsúlyozni kell, hogy míg a védelmi szabályozást a szakmai dimenzió jelentős mértékben meghatározza, addig másik oldalról a jogi szabályozásra a tágabb értelemben vett nemzeti jogrendszer is jelentős – és sok esetben a védelemszakmai törekvéseket megszűrő, módosító – hatást gyakorol. Fontos mindezek mellett azt is rögzíteni, hogy a nemzetállami szabályozási szintre a nemzetközi jogi dimenzió is hatással van, igaz, államonként eltérő mértékben. Az új típusú biztonsági kihívások és általában a 21. század fenyegetései

[18] E tekintetben kiemelendő, hogy a vizsgált európai államokat a kis tradicionális demokráciák, a nagy tradicionális demokráciák és a posztautokrata demokráciák közé sorolta be, ezzel is hangsúlyozva a nemzeti, ezen belül a történelmi, kulturális és geopolitikai sajátosságok fontosságát, azaz a komplexitás sajátos leképződését. Lásd Georg Nolte: *European Military Law Systems.* Berlin, De Gruyter Rect, 2003.

A nemzeti sajátosságok fontossága persze a magyar jogi és államtudományi gondolkodásban is ismert. A mintakövetés kapcsán Concha Győző több mint száz esztendeje úgy fogalmazott, hogy „Ha az egyik nemzet nem érezhet egészen úgy, mint a másik, egyénisége feláldozása nélkül, saját életszükségleteinek kell a kutatásra is ösztönözni, saját eszével kell gondolkodnia is; nem veheti át készen más nemzetek gondolkodása legmagasabb virágának, tudományának eredményeit, nem lehet merőben kölcsönző." Concha Győző: *Politika I. Alkotmánytan.* Budapest, Grill Károly Könyvkiadó vállalata, 1907, IX. o.

terén ugyanis az egyes államok nemzetközi jogi rendelkezésekhez, illetve azok értelmezéséhez való viszonyában jelentős kilengések is tapasztalhatók. Ezt éppúgy befolyásolják az adott állam nemzetközi hatalmi attribútumai, mint a szövetségi vagy integrációs hovatartozása, illetve ezeken belül a nemzetközi politikai törekvései. Ennek megfelelően a nemzetközi jog és a nemzetállami szint relációjában azonosítható valamiféle harmonizációs igény a legtöbb nemzet által elfogadott szabályrendszerek tekintetében, másik oldalról azonban számos új jelenség megítélése tekintetében fragmentáltság is érződik, ami egy adott kérdés kapcsán pro és contra jelleggel is orientálhat egy nemzetállamot. Meglátásom szerint a kibertérben végzett különféle műveletek jogi megítélésére – kötelező érvényű nemzetközi szerződés és kiforrott gyakorlat hiányában – az utóbbi jellemző. Ez azonban nem jelenti azt, hogy ne lennének a nemzetközi jognak a nemzetállami szintű szabályozást meghatározó vonatkozásai, inkább csak azt tükrözi, hogy a nemzeti szintű szabályozásban van lehetőség a részletes kidolgozásra.

Mindezek alapján úgy vélem, hogy az egyes nemzetek vonatkozásában a kibertérműveleti képességek kialakítását, fejlesztését a kimunkált, az államszervezet vonatkozásában is reális, átfogó és mégis hálózatos megközelítésre épülő szakmai koncepcióknak oly módon kell meghatároznia, hogy ezek a szakmai igények idomuljanak elsődlegesen a nemzeti jogszabályi környezet kereteihez és lehetőségeihez, miközben másodlagosan a nemzetközi mintákra, megoldásokra és a formálódó nemzetközi jogi értelmezésre is kellő figyelmet fordítanak.

2. A JÓ KORMÁNYZÁS, A KOMPLEX BIZTONSÁG ÉS A MEGALAPOZOTT DÖNTÉSHOZATAL IGÉNYEINEK KAPCSOLATA A KIBERTÉRMŰVELETI KÉPESSÉGEKKEL

A 19. századtól érezhető, dinamikus technológiai, közlekedési, kommunikációs, illetve gazdasági fejlődés, valamint ezeknek a társadalomra gyakorolt hatása magával hozta az állami funkciók gyarapodását és differenciálódását. Ez értelemszerűen a jogi szabályozás szakterületi tagozódását, valamint mélységét és kiterjedését is érintette. Kiválóan szemlélteti ezt a változást a különféle ma már bevettnek számító, de történelmi távlatokban újszerű jogterületek – szociális jog, munkajog, agrárjog, környezetvédelmi jog, infokommunikációs jog stb. – kialakulása, fejlődése ebben az időszakban, illetve a hagyományos jogterületek korszakos változásai és kodifikációs nóvumai a büntetőjogtól a közigazgatási jogon át a polgári jogig. Államszervezeti oldalról ezt hazánkban a Magyary Zoltán által képviselt iskola is jól fémjelezte, dokhíva a figyelmet az állam szervezetének differenciáltsága mellett egyes működési problémákra vagy kihívásokra, valamint az eltérő állami szférák – például a haderő és a közigazgatás – sajátos kapcsolódásaira. Persze ez a fajta szintetizálás eltérő nézpontokból is értékelhető, hiszen a közigazgatási vezérkar körüli gondolkodás

a katonai vezérkari szemlélettel kapcsolódva egyik oldalról felfogható az államélet militarizálásaként, másik oldalról pedig az egyre összetettebbé váló biztonsági környezet miatti sajátos szinkronizálásként is. Példaként használva és nem megnyitva ezt a messze vezető vitát, a magunk részéről úgy gondoljuk, hogy bár a 20. század első felében a militarizálás domináns jellemző volt szerte a világban, hosszabb távon a történelem, különösen a komplex biztonság fogalmával ebben a megközelítésben egy szintetikus, ha úgy tetszik, interoperábilis és multidiszciplináris gondolkodás alapjait igazolta. Erre pedig érdemes lehet ma is példaként tekintetni mind a különféle ágazatok, szektorok, szakterületek szintetizált működtetése, mind pedig a gyakorlati-mindennapi államműködés mögött álló elemző-kutató kapacitások fontossága és hatékonysága kapcsán.

Mindazonáltal a történelem nagy távlataiban nézve a 19–20. századi fejlődési hullám – amit ma már jól tudjuk, hogy a digitalizáció hatványozott hatásokkal folytat tovább – egyértelműen egy rendkívül intenzív és rövid idő alatt lezajló fejlődési „robbanást" valósított meg. Ez pedig az újdonságok, az előnyök és a szükségszerű specialitások mellett odavezetett, hogy a 20. század végén és a 21. század elején okszerű igényként merült fel az állam hatékonyabbá tétele, azaz az állami folyamatok és struktúrák szisztematikus reformja. Ennek egyik gyűjtő gondolati sémája lett a jó kormányzás irányába való előrelépés az elmúlt évtizedekben.

Az állam és jog technikai és társadalmi változásokhoz való alkalmazkodása és egyben önfejlődése mellett azonban a valós idejű és globális kommunikáció, a valóban globális és digitalizált kapitalizmus, a fogyasztói társadalom számos hatása, illetve a közlekedés fejlődése folytán a világ rendkívüli mértékben felgyorsult a korábbiakhoz képest. Ehhez az állami működésnek és különösen a döntéshozatalnak is fel kell zárkóznia. Ez a gyorsabb döntési igény azonban a nagy fajsúlyú, stratégiai – évtizedes – időtávlatú és emellett a gyorsaságot megkövetelő célok és ügyek elegyével jellemezhető területeken, mint amilyen a védelem és biztonságszavatolás is, fokozott kihívásként jelentkezik. Ennek orvoslása jellemzően a szakterületekre, funkciókra, témakörökre specializált koordináció erősítésével, szakosított döntési fórumok kialakításával, illetve információfúziós központok[19] kiépítésével valósult meg a napi állami feladatellátás tekintetében. Ez a 21. századi fejlődés és környezetváltozás időbeli felgyorsulására adott reakciókat tükrözi, illetve az információmennyiség szelektálását segítő intézményi és egyes esetekben személyi megoldásokat.

[19] A téma kapcsán lásd Hódos László: Gondolatok a nemzeti hírszerző képesség koordinációjáért felelős szerv közjogi helyzetéről. *Szakmai Szemle,* 2018/4. szám, 5–16. o.; Urbán Attila: A koordinációs folyamatok intézményi hátterének evolúciója a magyar nemzetbiztonsági igazgatásban. *Nemzetbiztonsági Szemle,* 2020/1. szám, 5–32. o.; Márton Balázs: A NIBEK-től a Nemzeti Információs Központig. *Nemzetbiztonsági Szemle,* 2023/1. szám, 21–33. o.; Farkas Ádám: *A védelem és biztonság-szavatolás szabályozásának alapkérdései Magyarországon.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2022.

Emellett azt is látni kell, hogy a felgyorsult világ tovább erősíti azt a korábbi trendet, hogy a napi gyakorlati államműködés és a különféle kapcsolódó tudományok elméleti-rendszerező szemlélete távolodni kezdett egymástól. Ez a problémamegoldás és döntéshozatal terén a napi működés dinamikájába ágyazott, gyors, konkrét kihívásokra és tárgykörökre fókuszáló megoldási sémákat eredményez, ami addig tartható fenn hatékonyan, amíg a működést megalapozó technikai és környezeti tényezők jelentősen nem alakulnak át. Egy szisztematikus változási folyamat, illetve adott esetben egy korszakváltás időszakában azonban az előző időszak módszereinek és szemléleteinek töretlen alkalmazása idővel szükségképpen maladaptívvá és rendszerszinten inkonzisztenssé válik. Ez pedig az időben felül nem vizsgált megoldások váratlan alkalmazásakor visszaüthet, de a környezeti változások folyamatos elemző-rendszerező monitorozásával és a napi gyakorlattal lekötött igazgatási és döntéshozatali intézmények kutató-elemző támogatásával megelőzhető. Erre a NATO és az EU szintjén kiváló példákat is adnak a különféle kiválósági központok és más háttérintézmények, de számos transzatlanti felsőoktatási intézmény és think tank kutatási és javaslatkidolgozói törekvései, továbbá a szakosított reformbizottságok is. Ez az irány hazánkban sem ismeretlen, akár a jogalkotást segítő reformbizottságok, akár a Mádl Ferenc Összehasonlító Jogi intézet felállítása révén. A megközelítés és intézményi háló azonban még nem tekinthető bevettnek, különösen a védelmi szférában, mivel helyette részlegesen lefedve a funkciót, különféle – döntően a gyakorlati szakemberekre és egy-egy kutatóra építő – munkacsoportok és tanácsok funkcionálnak.

Ahhoz tehát, hogy a kibertérműveleti képességek kialakításának, illetve fejlesztésének szabályozási és állami alapkérdéseiről kellő körültekintéssel gondolkodhassuk, szükséges az is, hogy a kérdést a nemzetállami szabályozás fent írt jelentőségére figyelemmel a jó kormányzás, továbbá a hatékony és gyors állami döntéshozatal megvilágításában is értelmezzük.

A *jó kormányzás* és vele a kormányzati teljesítmény mérhetősége és ezáltal javíthatósága az elmúlt évtizedekben elfogadott és fejlesztendő kérdésévé vált a nyugat-európai államszervezésnek és a hazai államtudományi gondolkodásnak is.[20] Ezek

[20] A téma kapcsán lásd Kaiser Tamás – Kis Norbert (szerk.): *A jó állam mérhetősége.* Budapest, Nemzeti Közszolgálati Egyetem, 2014; Kaiser Tamás – Bozsó Gábor: Az államközpontú kormányzás koncepciójának és mérhetőségének főbb aspektusai. *Államtudományi Műhelytanulmányok*, 2016/22. szám; Kaiser Tamás (szerk.): *A jó állam nagyító alatt: speciális jelentések A-tól V-ig (az adóbürokráciától a versenyképességig).* Budapest, Dialóg Campus Kiadó, 2016; Patyi András: Good Governance and Good Public Administration. *Public Governance Andministration and Finance Law Review in the European Union and Central Eastern Europe,* 2016/1. szám 1–14. o.; Stumpf István (szerk.): *Erős állam – alkotmányos korlátok.* Budapest, Századvég Kiadó, 2014; Matthew Andrews: *Good Government Means Different Things in Differenc Countries.* Harvard – John F. Kennedy School of Government, Faculty Research Working Papers, RWP08-068, 2008; John Graham – Bruce Amos – Tim Plumptre: *Principles for Good Governance in the 21st Century.* Ottawa, Institute on Governance – Policy Brief No. 15., 2003.

a kormányzás, illetve az állam tudományos elemzése terén megcélzott holisztikus, általános eredményekre vezetnek, azonban fontos, hogy a jó kormányzás égisze alatt megjelenő törekvések és kritériumok a védelem terén is leképeződjenek. E tekintetben persze figyelemmel kell lenni a fogalom „ideologikus" kettősségére is, „annál is inkább, mert Nyugat-Európában is a »jó kormányzás« kétféle felfogásának hívei mérik össze érveiket: az állam kitüntetett szerepéről lemondó neoliberálisok (good governance) az állam megerősítésében gondolkodókkal (good government) találják szembe magukat".[21] Az előbbi az állam szerepének megerősítése helyett az államon kívüli szereplők súlyát hangsúlyozza, és az államot elsősorban a jó kormányzás feltételeinek megteremtőjeként, de nem feladatainak megvalósítójaként fogja fel.[22] „Az államtalanítás híveivel szemben megfogalmazódó good government koncepció viszont éppen arra támaszkodik, amiről a rivális gyakorlat lemond. A modell szerint az állam nemcsak a jó kormányzás feltételeinek megteremtésében vállal szerepet, de a jó kormányzás feladatait is magára kell vállalja."[23] Ez utóbbinak a gazdasági válság, illetve a negatív elmozdulásokon átesett biztonsági környezet is erős érveket adott, hiszen a jó, hatékony, fejlődő társadalmi és gazdasági működéshez a megfelelő szabályozó, koordináló, felügyelő képességű aktornak – az államnak – ezeken túlmenően egyértelműen és korszerűen kell szavatolni a rendezett működéshez és fejlődéshez szükséges biztonságot és stabilitást is. Ez a vonatkozás pedig már egyértelműen hozzákapcsolja a védelemhez a jó kormányzás gondolatkörét. A digitalizáció társadalom- és gazdaságformáló, illetve biztonsági jelentősége miatt tehát a kibertérműveleti képességek fejlesztése kapcsán is fontos számolni a jó kormányzás követelményrendszerével és gondolati sémáival.

A jó kormányzás témánkra való átültetése, értelmezése érdekében talán a legjobban megragadható irányt a rossz kormányzás néhány jellemzőjének, mint ellensúlyozandó, kieszközölendő vonásoknak az áttekintése adhatja. Stumpf Istvánnak a rossz kormányzás fő indikátorairól írt gondolatai közül mindenképp megragadhatók a következők: (1) a kormányzás tartalmi, szakmai kérdései háttérbe szorulnak a politikai és személyi vonatkozásokkal szemben, (2) a politika sajátos logikája korlátozza a szakpolitikai koncepciók érvényesülését, (3) az egydimenziós logika fokozza a problémákat, (4) a célok és a vízió hiánya összekapcsolódik az eszközök válságával, (5) a struktúrák radikális átalakítása kaotikus eredményekhez vezet.[24] Ezek azok a főbb vonatkozások, amelyeket mindenképp kerülni kell a jó kormányzás érdekében, különösen az olyan újszerű és átfogó kihívásokat hordozó fejlesztési

[21] Stumpf István: A „jó kormányzás" két értelme. Avagy a demokratikus kormányzás programja és feltételei. In Stumpf István (szerk.): *Erős állam, alkotmányos korlátok.* Budapest, Századvég Kiadó, 2014, 68. o.

[22] Vö. Stumpf: i. m. (2014), 69–75. o.

[23] Stumpf: i. m. (2014), 75. o.

[24] Vö. Stumpf István: Neoweberi állam és jó kormányzás. Avagy mit tennél, ha te volnál az állam? In Stumpf István: *Erős állam, alkotmányos korlátok.* Budapest, Századvég Kiadó, 2014, 98–100. o.

területek kapcsán, mint amilyen a kibertérműveleti képességek fejlesztése, vagyis a tág értelemben vett információ- és kiberbiztonság.

A rossz kormányzás ezen torzulásainak elkerülésére az egyik lehetséges irány a neoweberiánus államfejlesztés gondolata, ami mind a funkciók, mind a struktúrák, mind a személyek és képességek terén a fejlesztés felé mutat. Ennek persze a fő megvalósulási mintáját a gazdaságfejlesztő államok adják, azonban az ott elvárt magas színvonalú, jól szervezett, koherens apparátus, a meritokratikus kiválasztás, illetve az állami és a magánszféra megfelelő együttműködése[25] – sajátosságok mellett persze, de – értelmezhető a védelem terén is. A fenti okfejtésünk ugyanis, amely a szakmai, a nemzeti jogi és a nemzetközi jogi keretek összehangolása felé mutat, jól illeszthető ehhez a sémához. A Stumpf István által hangsúlyozott neoweberi jellemzők sora felhívható itt (1) az állam szerepének újragondolásától és megerősítésétől, (2) a normativitás erősítésén és megújításán, (3) a közszolgálat eszményének helyreállításán és revitalizálásán, illetve (4) a hatékony és szolgáltatói szemléletű feladatellátáson át, egészen (5) a közszolgálat professzionalizációjáig.[26] E tekintetben kiemelendő a jó kormányzás azon előfeltétele, hogy „a közigazgatási döntés-előkészítés és ellenőrzés átfogó rehabilitációja, újjáépítése halaszthatatlan [...] az állam funkciói újragondolásának előfeltétele a közigazgatási szakmai tudásbázis megalkotása...".[27] Ennek átfordítása a kibertérműveleti képességek fejlesztésére azt hozza magával, hogy szükséges egy olyan multidiszciplináris szakmai-tudományos szakapparátus kialakítása, amely a stratégiai fejlesztést és kialakítást a döntés-előkészítés szintjén tudja támogatni, majd a jövőbeni korrekciókat sokrétű szakmai szempontok mentén képes lesz megalapozni. Másrészről a fentiek egy ilyen szakértő-kutató képesség kialakítása mellett szükségessé teszik

- a kibertérműveleti képességek beillesztését az állam változó feladatairól kialakítandó koncepcióba, stratégiába;
- az információ- és kiberbiztonság, valamint az ezzel összefüggő védelmi feladatokat ellátó állami funkciók szabályozásának megújítását, megerősítését, hogy a védelem egyszerre legyen korszerű, de jogállami és garanciális szemléletű;
- olyan közszolgálati életpálya- és működési modell kialakítását, amely a kibertérműveleti képességekkel és a komplex biztonsági környezettel összefüggő sajátos szaktudású apparátust is hivatásszerűen képes megtartani, motiválni, sőt a professzionalizáció érdekében továbbképezni; valamint
- a hatékony – de szakmai és biztonsági okokból hálózatos – képességkialakítás mellett egy olyan eljárásrend kialakítását, amely a civil társadalom számára is támogatható.

[25] Vö. Stumpf: i. m. (2014), 112–114. o.

[26] Vö. Stumpf: i. m. (2014), 114–118. o.

[27] Stumpf István: A jó kormányzás felé. In Stumpf István (szerk.): *Erős állam, alkotmányos korlátok.* Budapest, Századvég Kiadó, 2014, 148. o.

A jó kormányzás elvrendszerének terjedését és fontossá válását nagyban erősítették a valós idejű és gyorsan változó biztonsági kihívások is. Ezek mielőbbi kezelése érdekében *a kormányzati, illetve a tágabb értelemben vett közjogi döntéshozatal gyorsítása* egy olyan alapvető igény, amely az adott védelmi, illetve szakmai kérdések tekintetében a funkcióellátás teljes vertikumát érinti a tervezés és felkészítés fázisától az ügyeleti és készenléti szolgálatok, illetve szakállományok működésén keresztül egészen a felső szintű javaslattételig és döntéshozatalig. A kibertérműveleti tevékenységek körében ez a gyorsasági igény egyértelműen azonosítható, sőt megkerülhetetlen. Fontos azonban, hogy a kibertér biztonsága és biztonság érdekében történő alkalmazása, sőt ennél továbblépve a gazdasági és társadalmi jólétet és fejlődést serkentő hatásainak szavatolása érdekében nem csak a gyors reagálás kérdéseire kell fokozott figyelmet fordítani az állami szerepvállalás során. Az információs térrel összefüggő fejlődés szükségképpen korszakos változást hoz, és érinti a legtöbb viszonyrendszert jelen tapasztalataink szerint. Ez pedig sajátosan kapcsolódik össze a komplex biztonság sokrétűségével, valamint a biztonsági környezet negatív változásaival szembeni ellenálló képesség igényével is.

A biztonsági közeg komplexitása önmagában fokozódó együttműködést és jobb reagáló képességet feltételez az állam rendszeriben és hagyományos szabályozási területein is. A kibertér mellett az elmúlt évek különféle kihívásai és fenyegetései éppúgy válaszokat követeltek a büntetőjogtól[28], mint a közigazgatástól[29] vagy épp a védelmi szférától. Ezt a sokrétű hatásteret – amit a komplex biztonság maga jelent a korábbi szakterületek szerint tagoló biztonságképpel szemben – pedig a digitalizáció tovább erősíti és dinamizálja. Ennek eredményeként a kibertérműveleti képességek fejlesztése, szabályozása, szervezése és irányítása terén szoros szinergia kell az állam és jog „civil" vonatkozásaival, illetve a hagyományos védelmi szféra különféle ágazataival. Fontos, hogy ez a szemléletmódban is megjelenjen, vagyis a kibertérműveleti terület nyitott tudjon lenni a különféle kapcsolódó szektorok sajátosságai-

[28] A téma kapcsán példaként lásd Bartkó Róbert: *Az irreguláris migráció elleni küzdelem eszközei a hazai büntetőjogban.* Budapest, Gondolat Kiadó, 2020; Bartkó Róbert (szerk.): *A terrorizmus elleni küzdelem aktuális kérdései a XXI. században.* Budapest, Gondolat Kiadó, 2019; Kovács-Szépvölgyi Enikő (szerk.): *Kihívások a büntetőjogi jogalkotás terrénumában a 19–21. században. Külföldi minták és nemzeti megoldások.* Budapest, Gondolat Kiadó, 2022; Ambrus István: A 21. századi modernizációra adható büntetőjogi válaszok. *Ügyészek Lapja,* 2019/6. szám, 5–12. o.

[29] Lásd Balázs István – Hoffman István: A közigazgatási jog rezilienciája – koronavírus idején. In Gárdos-Orosz Fruzsina – Lőrincz Viktor Olivér (szerk.): *Jogi diagnózisok: a COVID-19-világjárvány hatásai a jogrendszerre.* Budapest, L'Harmattan Kiadó – MTA Társadalomtudományi Kutatóközpont, Jogtudományi Intézet, 2020, 45–65. o.; Bándi Gyula: Fenntartható fejlődés, reziliencia és közigazgatás. In Fazekas Marianna (szerk.): *Gazdaság és közigazgatás. Tanulmányok Ficzere Lajos tiszteletére.* Budapest, ELTE Eötvös Kiadó, 2015, 17–26. o.; Lapsánszky András: A COVID-19 járvány hírközlési vonatkozásai piaci és közigazgatáselméleti szempontból. *Jog Állam Politika,* 2022/különszám, 291–304. o.; Rixer Ádám (szerk.): *A járvány hosszútávú hatása a magyar közigazgatásra.* Budapest, Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar Lőrincz Lajos Közjogi Kutatóműhely, 2021.

ra, de fordítva is elmondható legyen, hogy a „civil" szektorok és a konvencionális védelmi ágazatok is transzformálják gondolatiságukba és működésükbe a kiberbiztonsági szemlélet sajátosságait.

Ez a fajta szemléleti és működési kölcsönhatás azonban más megvilágításban is érvényesítést sürget. Ez pedig az állami-társadalmi együttműködés. A digitális tér / kibertér decentralizáltsága és társadalmi-gazdasági kiterjedtsége miatt ugyanis a biztonság csak akkor szavatolható, ha abban a nem állami szereplők is aktívan részt vesznek, és az állami szereplők ezt a folyamatot segítik, illetve a hagyományos állami védelmi és biztonsági érdekek mentén történő alkalmazással megóvják. A civil-állami kooperáció fokozása azonban jelentős kihívás, különösen védelmi-biztonsági megközelítésben, mivel e funkciók alapvető jellemzője eddig a teljes állami dominancia volt. Az ehhez kapcsolódó, jellemzően imperatív-kényszerítő-tiltó szabályozási és igazgatási megoldások pedig önmagukban nem tudnak kellően hasznos megoldásai lenni egy reziliens és biztonsági értelemben is fenntartható kibertéri működésnek az információs társadalom korában. A védelmi funkciókat hagyományosan jellemző kemény eszközök mellett fontos, hogy az állam a kibertérműveleti képességeinek fejlesztésével összhangban fokozott hangsúlyt fektessen azokra a tevékenységekre, amelyek a biztonságtudatosítást, az állami-társadalmi együttműködést, illetve a nem állami szférában felmerülő tapasztalatok, igények és koncepciók hatékony és valós becsatornázását segíthetik. Ennek már több nemzetközi és külföldi példája[30] is azonosítható, amelyek erősödése és hazai meghonosítása is szükségszerűnek tűnik a jövőre nézve.

***

A különféle védelmi ágazatok korszerű és hatékony, a hálózatos felépítés mellett is együttműködésre képes kialakítása tekintetében egyértelműen látható, hogy a feladat aktuális és sürgető. Ennek rendszerszerű kialakítása és napi feladatokkal, kihívásokkal való egyensúlyba hozása azonban hosszabb távú és a mindennapi gyakorlati igazgatási funkciókon túli képességeket és intézményeket is szükségessé tesz.

A digitalizáció jelentősége, társadalmi, gazdasági és nem utolsósorban biztonsági hatásainak korszakos fontossága abba az irányba mutat, hogy a kibertér biztonságát és védelmét garantálni hivatott nemzeti kibertérműveleti erők kialakítása nem egy aktuálisan teljesítendő és aztán elfelejthető feladat, hanem egy olyan új képességfejlesztési kihívás minden védelmi ágazatban, amely egy a 21. századi biztonság-

[30] A téma kapcsán lásd Udo Helmbrecht et al.: *Cybersecurity cooperation.* Herakleion, European Union Agency for Network and Information Security, 2013; Liina Areng: *Lilliputian States in Digital Affairs and Cyber Security.* Tallinn, NATO CCD CoE Tallinn Paper No. 4., 2014; Petruska Ferenc – Vikman László: Egy formabontó hírszerzési nyilatkozat a jogi sérülékenységek szempontjából. *Military and Intelligence CyberSecurity Research Paper,* 2021/4.

hoz nélkülözhetetlen, új képesség- és funkcióösszesség létrehozásával azonosítható. Ennek jelentőségét tovább fokozza, hogy a kiberbiztonság hatékony építése elképzelhetetlen a széles körű nem állami szerepvállalás és támogatás nélkül, amely az információs társadalom rezilienciájának sokrétű kialakításával kapcsolható össze.

Ahhoz, hogy ezen képességek kialakítása, illetve fejlesztése hosszú távon is eredményes és a kor kívánalmainak megfelelő legyen, és ennek részeként a költségvetési forrásokat is hatékonyabban használja fel, szükséges, hogy az komplex módon, a képességek generálása és szervezeti kereteik kialakítása mellett a megfelelő szabályozás kidolgozásával és folyamatos megújításával történjen, méghozzá minden érintett védelmi ágazatra kiterjedő módon és azok együttműködésével. Fontos azonban az is, hogy a komplex biztonság korában a komplexitáshoz igazodó szemléletmódot alkalmazzunk, hiszen a leegyszerűsítés egy bonyolult világban bizonytalan eredményekre vezethet. Barabási Albert-László kiváló érzékkel mutatott rá ennek lényegére: „Sok XX. századi tudományos kutatás hajtóereje volt az egyszerűsítés. A természet megértéséhez először az összetevőit kell megfejtenünk. A feltételezés az, hogy ha egyszer megértjük a részeket, akkor könnyű lesz az egészet felfognunk. Oszd meg és uralkodj; az ördög a részletekben van. Ezért évtizedeken keresztül arra kényszerültünk, hogy a világot alkotóelemein keresztül lássuk. [...] Közel vagyunk ahhoz, hogy majdnem mindent tudjunk, amit a részekről tudni lehet. A természet egészének megértésétől azonban ugyanolyan messze vagyunk, mint bármikor korábban. Az újra összerakás tényleg sokkal nehezebb, mint azt a tudósok gondolták. Az ok egyszerű. Az egyszerűsítést erőltetve beleütköztünk a komplexitás kemény falába. Megtanultuk, hogy a természet nem egy jól megtervezett összerakós játék, amely csak egyféleképpen rakható össze. [...] Manapság egyre inkább felismerjük, hogy semmi nem történik elszigetelten. A legtöbb esemény és jelensége része egy komplex, univerzális kirakós játéknak, amelynek sok-sok darabja egymással kapcsolatban és kölcsönhatásban áll, egymást befolyásolja. Elkezdtük belátni, hogy egy kis világban élünk, amelyben minden minden mással össze van kapcsolva. Egy most születő forradalomnak vagyunk a tanúi, melynek során a különböző tudományágak tudósai felfedezik, hogy a komplexitásnak szigorú szerkezete van. Elkezdtük megérteni a hálózatok fontosságát."[31]

A komplexitás talaján állva tehát keresni kell egy olyan irányt, amely a kiberteret és annak biztonságát rendszerként közelíti meg, de emellett az egyes hagyományos – mégis a kibertér által érintett – szférák tekintetében is előmozdítja az infokommunikációs környezet miatt szükséges fejlesztéseket. Előbbi átfogó keret lehet a tág értelemben vett információ- és kiberbiztonság, míg utóbbi szükségessé teszi az egyes védelmi funkciókon belül az adott feladatellátás sajátosságaihoz igazodó ki-

[31] Barabási Albert-László: *Behálózva.* Budapest, Libri Kiadó, 2003, 12–13. o.

bertérműveleti képességek kialakítását a kiberbűnüldözéstől, a kiberhírszerzésen és -elhárításon át egészen a katonai kibervédelemig.[32]

Egy ilyen összetett, széles körű, mégis rendszerszinten záródó fejlesztés és megújítás komoly szakmai és nem utolsósorban tudományos megalapozást igényel. A kiberbiztonság és -védelem sajátosságaiból adódó, széles körű, sokrétű, multidiszciplináris szakmai igények és követelmények összehangolása már önmagában is jelentős feladat, hiszen a szűk értelemben vett védelmi szakkövetelmények mellett a tágabb IT szakmaiságnak, sőt a kapcsolódó összes szakterületnek és az innovációs célkitűzéseknek is megfelelően érvényesülnie kell. Ezeket a szakmai kritériumokat azonban össze kell hangolni a jog sajátosságaival, illetve kapcsolódó fejlesztési igényeivel, majd a szélesebb körű „civil" szektorok sokaságának specialitásaival, elvárásaival és igényeivel.

Egy ilyen előkészítő folyamat szükségképpen a védelmi és ezen belül a kibervédelmi funkciók sajátos igényei mellett is beépítendők az állam fejlesztésének tágabb láncolatába. A kibertérműveleti képességek kialakításánál tehát érdemes a jó kormányzás követelményeit is szem előtt tartani mind az aktív, műveleti, mind a támogató képességek és keretek kialakításánál. A képességgeneráláson túl vizsgálandó azonban a terület feletti kormányzati-politikai koordináció és irányítás szisztémája, valamint a rendszerszintű és stratégiai távlatú javaslatok kidolgozásához szükséges sajátos háttérintézmények létesítésének, fenntartásának és megerősítésének kérdésköre is. Az, hogy ebben a folyamatban meg kell és lehet őrizni korábbi jó gyakorlatokat, biztonsággal kijelenthető. Legalább ilyen, de inkább nagyobb bizonyossággal állítható azonban, hogy tudnunk kell alkalmazkodni a korszakos változáshoz is, hiszen ahogy Zygmunt Bauman a globalizáció viszonylatában megfogalmazta: „…a mozdulatlanság nem reális alternatíva egy állandóan változó világban."[33]

[32] Fontos azonban itt kiemelni, hogy a védelem szó ez esetben is az adott nemzet, állam, szövetség érdekeinek komplex védelmét és érvényesítését jelenti, vagyis a köznapi értelemben vett támadó cselekményekre, képességekre is kiterjed. Ezzel kapcsolatban bővebben lásd Farkas: i. m. (2018); Farkas Ádám: Az állam védelmi kötelezettségeinek egyes kortárs aspektusai. *Jogelméleti Szemle*, 2018/4. szám, 53–70. o.

[33] Zygmunt Bauman: *Globalizáció*. Szeged, Szukits Könyvkiadó, 2002, 17. o.

VIKMAN LÁSZLÓ

Gondolatok a kiberbiztonsági stratégiák fejlesztésére vonatkozó nemzetközi útmutató kapcsán

Kiberbiztonsági stratégiával az Európai Unió minden tagállama rendelkezik már, sokuk esetében második, sőt harmadik iterációjánál tart az információs társadalmat és gazdaságot alapvetően meghatározó infokommunikációs szféra nemzeti szabályozási, adminisztratív és fejlesztési kereteit megfogalmazó dokumentum.[1] Ez azonban nem jelenti azt, hogy a kiberbiztonsági stratégiaalkotás folyamata már nyugalmi szakaszba érkezne, mivel számos képességfejlesztés és azok intézményi és szabályozási lekövetése, illetve az infokommunikáció és különösen a kibertér 21. századi biztonságban betöltött szerepe[2] újabb és újabb kihívások elé állítja ezt a szakpolitikát. Ehhez is kötődve, a következő időszakban az EU-tagállamok egyik fontos mércéje és a stratégiák revíziójának háttere lesz az Európai Bizottság által kiadott, „Digitális iránytű 2030-ig: a digitális évtized megvalósításának európai módja"[3] című stratégia. Ennek néhány – részben figyelemhívási céllal önkényesen kiválasztott – fontos megállapítását érdemes talán felsorolni:

- A következő időszakban jelentős lehet a dezinformáció demokratikus társadalmainkra gyakorolt hatására.
- Az EU gyakran nem uniós alapú technológiáktól való fokozott függése, és a tény, hogy a digitális csúcstechnológiákat többnyire az EU-n kívül fejlesztik, egyre komolyabb versenyhátrány és egyben biztonsági kockázatok forrása is.

[1] Lásd a tagállamok stratégiáit egy helyen közlő tematikus oldalt, az ENISA gondozásában: https://www.enisa.europa.eu/topics/national-cyber-security-strategies.

[2] A téma kapcsán lásd Merle Maigre: Cyber threat actors: how to build resilience to counter them. *Hybrid CoE Paper*, 2022/11. szám; Antonio Missiroli: Geopolitics and strategies in cyberspace: Actors, actions, structures and responses. *Hybrid CoE Paper*, 2021/7. szám; William E. Leigher: Cyber conflict in a hybrid threat environment: Death by a thousand cuts. *Hybrid CoE Paper*, 2021/10. szám; Ben Buchanan: *The Hacker and the State. Cyber Attacks and the New Normal of Geopolitics.* Cambridge, Harvard University Press, 2020; Kelemen Roland: Radikalizálás, dezinformálás és tömegpszichózis modern köntösben: a hibrid konfliktus kibertérben. *Jog Állam Politika*, 2021/3. szám, 71–85. o.; Kelemen Roland – Farkas, Ádám: To the Margin of the Theory of a New Type of Warfare: Examining Certain Aspects of Cyber Warfare. In Szabó, Marcel – Gyeney, Laura – Láncos, Petra Lea (szerk.): *Hungarian Yearbook of International law and European Law (2019).* Den Haag, Eleven International Publishing, 2020, 203–226. o.; Farkas Ádám: A kibertér műveleti képességek kialakításának és fejlesztésének egyes szabályozási és államszervezési alapvonalai. *Jog Állam Politika*, 2019/2. szám, 63–79. o.

[3] Brüsszel, 2021.3.9. COM(2021) 118 final.

- A polgárokat, kkv-kat, a közszférát és a nagyvállalatokat kiszolgáló digitális infrastruktúra nagy teljesítményű számítástechnikát és átfogó adatinfrastruktúrát igényel.
- Európa digitális vezető szerepe és globális versenyképessége az erős belső és külső konnektivitástól függ, és a közösség nemzetközi szerepvállalását is meg kell határoznia.
- Az EU-nak világviszonylatban élen kell járnia a kvantumszámítógépek fejlesztése terén, többek közt azért, mert a kvantumbiztonságos kommunikációs rendszerek megóvhatják az érzékeny kommunikációt.
- A digitális transzformációnak lehetővé kell tennie továbbá a modern és hatékony igazságszolgáltatási rendszereket, a fogyasztói jogok érvényesítését és az állami fellépés, többek között a bűnüldözési és nyomozati kapacitások hatékonyságának növelését is.
- Fontos cél olyan, mesterséges intelligencián alapuló biztonsági műveleti központok hálózatának kiépítése, amelyek képesek kellő időben észlelni egy kibertámadás jeleit, és proaktív fellépést tesznek lehetővé a nemzeti és uniós szintű közös kockázati felkészültség és reagálás javítása érdekében.

A példaként felhozott témákból érezhető, hogy a kiberbiztonsági stratégiák rendszeres felülvizsgálata, a változó fenyegetésekhez igazítása, a technológiai innováció okozta szükségszerűségből fakadó frissítése visszatérő, ciklikus feladat, amelyhez számos módszertani, „best practice"-alapú vagy éppen összehasonlító jellegű útmutatót vehetnek igénybe az új iránymutatások kidolgozásával megbízott szakemberek.[4]

Ebben a fejezetben röviden egy ilyen útmutató főbb javaslatait szeretném bemutatni, aminek különlegességét az elkészítésében részt vevő szervezetek sokszínűsége, a közreműködő szakemberek globális és diverz háttere adja. Ennek köszönhetően esetleg olyan perspektívák és gondolatok forrása lehet, amelyek túlmutathatnak Magyarország esetében az olyan alapvető viszonyítási pontjainkon, mint az Európai Unió, esetleg a NATO,[5] illetőleg az egyes államok megoldásainak áttekintése.[6] Be

[4] Példaként lásd Claire Vishik – Mihoko Matsubara – Audrey Plonk: Key Concepts in Cyber Security: Towards a Common Policy and Technology Context for Cyber Security Norms. In Anna-Maria Osula – Henry Roigas (szerk.): *International Cyber Norms: Legal, Policy & Industry Perspectives.* Tallinn, NATO CCD COE Publications, 2016; Carol A. Siegel – Mark Sweeney: *Cyber Strategy – Risk-Driven Security and Resiliency.* Boca Raton, CRC Press, 2020.

[5] Lásd Kovács, László: Cyber Security Policy and Strategy in the European Union and NATO. *Land Forces Academy Review*, 2018/1. szám, 16–24. o.

[6] E körben lásd például Farkas Ádám: Kibertér művelet: hírszerző, rendészeti és katonai műveletek elegye? Gondolatok az angol National Cyber Force kapcsán. *Military and Intelligence CyberSecurity Research Paper* 2021/1. szám; Vikman László: A német kiberbiztonsági szisztéma áttekintése. Szervezeti keretek, különös tekintettel a nemzetbiztonsági szolgálatok és a hadsereg szerepére és kapcsolatára, valamint a szabályozási háttér alakulására. *Military and Intelligence CyberSecurity Research Paper*,

kell ugyanis látni, hogy a digitális környezet dinamikus fejlődése és az emberiség információs korszakba lépése komoly társadalmi-politikai és egyben biztonsági változások sorát idézte elő, illetve idézi elő a jövőben. A szervezett állami és társadalmi működés pedig e változások lekövetése miatt azok mértékhez igazodó szabályozási kérdések sorával is szembe néz a következő időszakban, ami a stratégiai horizontot is érinti.

1. AZ NCS GUIDE[7] – ÚTMUTATÓ EGY NEMZETI KIBERBIZTONSÁGI STRATÉGIA KIDOLGOZÁSÁHOZ

A 2021-ben publikált útmutató – melynek első verzióját 2018-ban adták ki – elkészítésében 20 kormányközi és nemzetközi szervezet, a privát szektor és az akadémiai szféra jelentős képviselői, továbbá különféle civil szervezetek szakértői működtek közre. Ezek közül – példálózó jelleggel – kiemelhető a kidolgozók sokrétűségét mutatva: az Európa Tanács, a Geneva Centre for Security Sector Governance (DCAF), a Deloitte, az International Criminal Police Organization (Interpol), az International Telecommunication Union (ITU), a Microsoft, a NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), a RAND Europe vagy a Világbank.

A dokumentum célja a nemzeti döntéshozók és szabályozásformálók számára segítséget nyújtani egy korszerű nemzeti kiberstratégia elkészítésében, amely figyelemmel van a kiberbiztonságra, kiberfelkészültségre és ellenálló képességre. A kiberbiztonság megteremtése összetett kihívás, amely magában foglal számos kormányzástechnikai, szabályozási, műveleti, műszaki és jogi aspektust is. Az útmutató küldetése, hogy kifejtse, rendszerezze és priorizálja ezeket a területeket létező és széles körben elterjedt modellezési és keretrendszerekkel. Mint ilyen, az útmutató szellemiségében egyértelműen rámutat arra, hogy a kiberbiztonság szavatolása szervesen illeszkedik abba a 21. századi biztonságot érintő nézetrendszerbe, amely a biztonságot és annak erősítését komplex és rendszerszerű megközelítéssel tartja csak helyesen megoldhatónak.[8]

2021/2. szám; Spitzer Jenő: A francia kibervédelmi és kiberbiztonsági rendszer egyes stratégiai aspektusai. *Military and Intelligence CyberSecurity Research Paper*, 2021/3. szám.

[7] Guide to Developing a National Cybersecurity Strategy (NCS Guide) (https://ncsguide.org/wp-content/uploads/2021/11/2021-NCS-Guide.pdf).

[8] Példaként lásd Nora Vanaga – Toms Rostoks (szerk.): *Deterring Russia in Europe.* Defence Strategies for Neighbouring States. London – New York, Routledge, 2019; Piotr Szymanski: *New Ideas for Total Defence. Comprehensive Security in Finland and Estonia.* Warsaw, Centre for Eastern Studies, 2020; Philipp Lange: Total Defence. How Germany should implement a whole-of-government national and collective defence. *Security Policy Working Paper*, 2018/2. szám; Farkas Ádám: *A totalitás kora? A 21. század biztonsági környezetének és kihívásainak totalitása és a totális védelem gondolatkísérlete.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2018; Farkas Ádám: *Az állam fegyveres védelmének alapvonalai.* Budapest, Katonai Nemzetbiztonsági Szolgálat, 2020.

Jelen mű célja áttekinteni és bemutatni az útmutató szellemiségét és újszerűségét, így elsődlegesen annak alapelvi jellegű felvetéseit érdemes kidomborítani, míg az útmutató első fő tartalmi egységében (Section 3. Lifecycle of a National no- curity Strategy) kifejtett, de egyébként nagyon is értékes és hasznos stratégia-életciklusra, kidolgozási metodikára nem térnék ki, egy fontos kivételtől eltekintve. Ez pedig a későbbi implementációban ideálisan nem érintett stratégiakidolgozási projektvezető függetlenségének és megfelelő felhatalmazásokkal való ellátásának kérdése, amely nélkül a kidolgozásban részt vevő szervezetek, érdekeltek között a szakmai alapú bizalom és egyensúly megbomolhat.[9]

Az útmutató elsősorban a kibertér polgári vagy „civil" védelmére – vagyis nem a katonai dimenzióra – koncentrál, és a következő két érdemi része olyan fő szervező alapelveket (Section 4 Overarching Principles) és jó gyakorlatokat (Section 5 National Cybersecurity Strategy Good Practice) ad meg, amelyek mindenképpen megfontolásra érdemesek egy kiberstratégia kidolgozási folyamatában, ezért ezeket legalább említés szintjén érdemes leltárba venni.

A fő alapelveket úgy fogalmazták meg, hogy egy előretekintő és holisztikus megközelítésű stratégia megformálásához adjanak vezérfonalat, és a kidolgozási folyamat egészében irányt mutathatnak, hiszen nem korlátozódnak egy-egy lépésre. A felsorolásuk sorrendjében is inkább logikai narratívát, mint hierarchiát kell keresni. Az optimális stratégiának

- világos összkormányzati és össztársadalmi víziót kell meghatároznia;
- a teljes digitális környezetet átfogó, mégis az adott ország körülményeihez és prioritásaihoz igazított elemzésből kell fakadnia;
- valamennyi érintett és érdekelt szereplő aktív részvételével kell készülnie, a szükségleteik és felelősségi körük meghatározásával;
- gazdasági és társadalmi fejlődést kell ösztönöznie, hogy maximalizálja az információs és kommunikációs technológiák hozzájárulását a fenntartható fejlődéshez és a társadalmi inkluzivitáshoz;
- meg kell felelnie az alapvető emberi jogokból származó követelményeknek, és tiszteletben kell tartania azokat;
- lehetővé kell tennie a kiberbiztonsági kockázatok hatékony menedzselését, és ösztönöznie kell a gazdasági és társadalmi tevékenységek rezílienciáját;
- alkalmaznia kell a lehető legmegfelelőbb rendelkezésre álló szabályozási megoldásokat a kitűzött célok elérésére, figyelembe véve az adott állam sajátos körülményeit;

[9] NCS Guide 16. o.

- a kormányzat legmagasabb szintjéről kell kiadni, innen elosztva a releváns szerepeket és felelősségi köröket, és rendelkezésre bocsátva a szükséges humán- és pénzügyi erőforrásokat;
- segítenie kell egy olyan digitális környezet kiépülését, amelyben az állampolgárok és a szervezetek megbízhatnak.

A kiberbiztonsági stratégia a társadalmi-gazdasági fejlődés számos területét érinti, és több tényező is befolyásolja a nemzeti kontextusban. Ezért a stratégia átfogó jellege és hatékonysága érdekében a szerzők olyan jó gyakorlatokra is tettek javaslatokat, amelyek segíthetik a nemzeti kontextusba illeszkedő dokumentum kidolgozását. Ezeket a javaslatokat csoportokba rendezve fogalmazták meg, és az egyes kidolgozó államok saját szervezetrendszerének, szabályozásának és infrastruktúrájának fejlettségétől is függ, hogy melyek alkalmazhatók.

1.1. fókuszterület: kormányzat

Biztosítani kell a legmagasabb szintű támogatást, továbbá a kormányzaton belüli és a szektorok közötti együttműködést. Létre kell hozni – ha lehetőség van rá, akár ágazatonként is – egy kompetens központi kiberbiztonsági szervezetet, allokálva a szükséges erőforrásokat. A stratégia végrehajtását lépésekre lebontott akcióterv kidolgozásával és ellenőrzésével kell megvalósítani.

1.2. fókuszterület: kockázatkezelés a nemzeti kiberstratégiában

A kiberfenyegetettség értékelését[10] és a kormányzási irányvonalakat a folyamatosan szélesedő kiberfenyegetési térképhez[11] kell igazítani. Meg kell határozni – ezzel egységesíteni – a kockázatmenedzsment megközelítéseket, valamint rögzíteni kell a kockázatkezelés egységes metodológiáját. Ki kell dolgozni szektorális kockázati profilokat, és a kiberbiztonsági szabályozás kidolgozásakor erre is figyelemmel kell lenni.

[10] Kiberfenyegetések értékeléséhez lásd Gregory Falco – Eric Rosenbach: *Confronting Cyber Risk – An Embedded Ensurance for Cybersecurity.* Oxford, Oxford University Press 2022, 41. o.

[11] A jövőbeni fenyegetésekhez, mint AI, közösségi média, adatvédelem, zero-trust hálózatok stb., lásd pl. Hamid Jahankhani – Liam M. O'Dell – Gordon Bowen – Danial Hagan – Arshad Jamal: *Strategy, Leadership, and AI in the Cyber Ecosystem – The role of digital societies in infromation governance and decision making.* London, Academic Press, 2021.

1.3. fókuszterület: felkészültség és rezíliencia

Ki kell alakítani eseménykezelő képességeket, kiberbiztonsági incidenskezelési és katasztrófaelhárítási terveket. Ösztönözni kell az információmegosztást, gyakorlatokat kell végezni, és ki kell értékelni a kiberbiztonsági eseményeket.

1.4. fókuszterület: kritikus infrastruktúrák és alapvető szolgáltatások

Ki kell alakítani egy kockázatkezelő megközelítést a létfontosságú rendszerelemek és alapvető szolgáltatások azonosítására és védelmére, olyan háttérszabályozással, amely átlátható felelősségi köröket ad meg. Meg kell határozni a minimális kiberbiztonsági alapkövetelményeket, piaci ösztönzőket kell kialakítani, és a privát és közszféra közt működőképes partnerkapcsolatokat.

1.5. fókuszterület: képesség és kapacitás építése, a tudatosság növelése

Stratégiai szemlélettel szükséges megtervezni a képességek és különösen ezek teherbírásának kialakítását. Ki kell építeni a kiberbiztonsági képzések kereteit, ösztönözni kell a munkaerő képzését. Koordinált kiberbiztonsági tudatosságnövelő programot kell indítani. Támogatni kell a kiberbiztonsági innovációt és kutatás-fejlesztést. Pályázatokat, támogatási programokat kell indítani a sérülékeny és forráshiányos szektorok és csoportok részére.

1.6. fókuszterület: törvényalkotás és részletszabályozás

Ki kell alakítani a kiberbiztonság és ehhez kapcsolódóan a kiberbűnözés és a digitális forenzikus terület nemzeti jogi keret- és részletszabályozását.[12] Védeni kell az emberi szabadságjogokat, ki kell alakítani a szabályok betartását ellenőrző compliance-mechanizmusokat. Ösztönözni kell a bűnüldözés releváns képességeinek fejlesztését, és a szervezetek közötti információcsere és közös munka alapjait jelentő eljárások bevezetését. Támogatni kell a nemzetközi kooperációt a kiberfenyegetések és kiberbűnözés elleni küzdelemben.

[12] A témához lásd pl. Damien Van Puyvelde – Aaron F. Brantly: *Cybersecurity – Politics, Governance and Conflict in Cyberspace.* Cambridge, Polity Press, 2019, 54. o.

1.7. fókuszterület: nemzetközi kooperáció

A kiberbiztonságot a külpolitika fontos elemeként kell kezelni és ehhez kell igazítani a hazai és nemzetközi erőfeszítéseket.[13] Részt kell venni a nemzetközi eszmecserékben és a közösen kialakított irányelvek implementációjában.[14] Ösztönözni kell a hivatalos és informális kooperációt a kibertérben, és a nemzetközi kooperációhoz szükséges képességek kiépítését, növelését.

2. ÉSZREVÉTELEK ÉS GONDOLATOK AZ ÚTMUTATÓ KAPCSÁN

Bármely nemzeti stratégia ritkán áll egymagában, mivel az adott ország kormánya által kialakított szakpolitikák közvetlen manifesztációi, fejlesztésük csak más területekre tekintettel lehetséges.[15] Az állami költségvetés kialakítása, az egyes társadalmi érdekek megjelenítése a táblázat soraiban az erőforrások és lehetőségek végessége miatt egy zéró összegű játszma eredménye, a prioritások meghatározásával lehet garantálni azt, hogy ami fontos, az mindenképpen kapjon erőforrást. Ezért az útmutató is több esetben hangsúlyozza, hogy a stratégiát a nemzeti sajátosságok és a már meglévő képességek ismeretében kell kialakítani.[16] Emellett nem szabad elfelejteni, hogy a redundanciák a biztonság és így a kiberbiztonság területén sem feltétlenül

[13] A kiberkonfliktusok jövőjéhez lásd Christoper Whyte – Brian Mazanec: *Understanding Cyber Warfare – Politics, Policy and Strategy.* New York, Routledge, 2019, 272. o.

[14] A nemzetközi kibertér és kiberbiztonság területén a nemzetközi jog vonatkozásában is bőven akadnak fejleszthető aspektusok, nem véletlen, hogy a leginkább elfogadott, témához kapcsolódó szakkönyv is már korábban meglévő nemzetközi szerződésekből, jogelvekből, szokásjogi szabályokból épített analógiákkal operál túlnyomórészt: Michael N. Schmitt (szerk.): *Tallinn Manual 2.0 On the International Law Applicable to Cyber Operations.* Cambridge, Cambridge University Press, 2017.

[15] Ha Magyarországot tekintjük, a kiberbiztonság területét a következő – bizonyos vonatkozásokban egymásra is épülő – stratégiák közvetlenül érintik: 1139/2013. (III. 21.) Korm. határozat, Magyarország Nemzeti Kiberbiztonsági Stratégiájáról, 1838/2018. (XII. 28.) Korm. határozat, Magyarország hálózati és információs rendszerek biztonságára vonatkozó stratégiájáról, 1573/2020. (IX. 9.) Korm. határozat, Magyarország Mesterséges Intelligencia Stratégiájáról, valamint a végrehajtásához szükséges egyes intézkedésekről, 1163/2020. (IV. 21.) Korm. határozat, Magyarország Nemzeti Biztonsági Stratégiájáról, 1393/2021. (VI. 24.) Korm. határozat, Magyarország Nemzeti Katonai Stratégiájáról. A szóban forgó stratégiák mellett látni kell azt is, hogy a vonatkozó jogszabályi környezet alakítása, különösen a feladatrendszerek és felhatalmazások változása is komoly hatással lehet a stratégiákban meghatározottak megvalósítására.

Ezenfelül lényeges, hogy külön szakirodalma van már az egyes nemzeti kiberbiztonsági stratégiák összehasonlításának is, lásd pl. Scott N. Romaniuk – Mary Manjikian (szerk.): *Routledge Companion to Global Cyber-Security Strategy.* New York, Routledge, 2021.

[16] Az USA-ban a National Defense Authorization Act alapján, 2019-ben létrehozott Solarium Bizottság végzett kiterjedt háttérmunkát az USA kiberbiztonsági stratégia kidolgozásának előkészítéséhez, lásd Brandon Valeriano – Benjamin Jensen: *Building a National Cyber Strategy: The Process and Implications of the Cyberspace Solarium Commission Report.* In T. Jancárková – L. Lindström – G. Visky

jelentenek pazarlást, sőt a hálózatos elvű védekezés tekintetében komoly előnyökkel is járhatnak. Emellett az is igaz, hogy a megfelelő összkormányzati egyeztetéssel, az akciótervek alapján az előrehaladás rendszeres értékelésével, kontrollmechanizmusok alkalmazásával, az esetleges gyakorlati tapasztalatok feldolgozása eredményeként az esetlegesen valóban indokolatlan, vagy a lekötött erőforrásokkal arányban nem álló hozadékokkal párosuló „vadhajtások" korrigálhatók.

Néhány egyéb gondolat felvethető még, ami a meglévő szabályozási rend, intézményrendszer, aktuális fenyegetések tükrében hangsúlyt kaphat. Ilyenek például a következők:

- A digitális közegben működő közösségi média kapcsán az ellenérdekelt szereplők információs műveleteivel szemben hatékony eszközök kialakítására van szükség,[17] mivel az ilyen fenyegetések a társadalmi, diplomáciai és gazdasági – sőt szélsőséges esetben a katonai – kohéziót és cselekvőképességet is alááshatják.
- Az államműködés és ebből következően kormányzás, az irányítás és vezetés folytonossága legalább olyan fontos, mint a létfontosságú rendszerelemek és alapvető szolgáltatások működtetése, az ehhez szükséges infrastruktúrák biztosítása és ennek részeként szükséges mértékű és hálózatos szervezési elven nyugvó redundanciája alapvető biztonsági érdek.
- A kiberbiztonság összkormányzati tevékenység, de az egyes részterületek felelősei között adott esetben a feladatok és hatáskörök, felelősségi területek vonatkozásában lehetnek súrlódások, amelyek gyors és hatékony rendezésére megfelelő mechanizmusok és felhatalmazások szükségesek, hogy a gyors eseménykezelés minden esetben garantálható legyen, és a fejlesztések során se alakuljon ki a működést nehezítő egyensúlytalanság a nemzeti rendszer egészére vetítve.
- Az útmutatóban is hangsúlyozott állami és civil szféra közötti információcsere valóban ösztönzendő, de bizonyos adatok a minősített vagy üzleti titok jellegük, esetleg más ok miatt kizárólag a kezelésükhöz előírt csatornákon mozoghatnak, amihez a szükséges adminisztratív és műszaki háttér is biztosítandó,

– P. Zotz (szerk.): *13th International Conference on Cyber Conflict: Going Viral.* Tallinn, NATO CCD COE Publications, 2021.

[17] A téma kapcsán lásd Végh Károly: Információs és befolyásolási műveletek a nemzetközi jog „szürke zónájában". In Farkas Ádám – Végh Károly (szerk.): *Új típusú hadviselés a 21. század második évtizedében és azon túl. Intézményi és jogi kihívások.* Budapest, Zrínyi Kiadó, 2020, 191–212. o.; Quareshi Waseem Ahmad: Information Warfare, International Law, and the Changing Battlefield. *Forsham International Law Journal,* 2020/4. szám, 901–937. o.; Farkas Ádám – Spitzer Jenő: Az információs korszak és az állami rezíliencia egyes kérései. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok*, 2021/18. szám; Vikman László: A közműszolgáltatások és a reziliencia egyes kérdései, különös tekintettel a kiberbiztonságra. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok*, 2021/14. szám.

egyébként egyes kérdésekről csak absztrakt, konkrétumok nélküli egyeztetések folytathatók, ami a biztonságszavatolás konkrét végrehajtási szintjén képességcsökkenést eredményez.
- Az EU Iránytű is említi, hogy az EU-s érdekkörben történő kritikus fejlesztések kulcsfontosságúak, nincs ez másként nemzeti szinten sem, mivel a kereskedelmi megoldások biztonsági színvonala nem minden feladathoz megfelelő.

Az előzőekben áttekintett és felvetett gondolatokat egybevetve az is kiemelendő, hogy a legrészletesebb és mindenre kiterjedő stratégia és akcióterv is csupán annyit ér, amennyit ténylegesen végre is hajtanak belőle. Ahhoz, hogy az adott intézkedés hatást érjen el, szükséges az érintettek hozzáértése, szakértelme mellett azok hivatástudata és elkötelezettsége is, továbbá a biztonságtudatosság – feladatellátáson túlmutatóan – széles körű erősítése. Ekkor van ugyanis esély a célok irányába történő eredményes előrelépésre. Amellett, hogy az útmutató igényes részletességgel veszi végig a valóban tisztázandó témaköröket, legfontosabb értékeként a szerkesztők által alkalmazott rugalmas megközelítést, a jó gyakorlatokból leszűrt alapelvek rendszerezését tekinthetjük. Tudományos igényességét pedig jól jelzi, hogy az elmélyülést, az egyes résztémák részletes feltárását a dokumentum végén egy részletes és aktuális forrásgyűjtemény segíti, ami a témával kapcsolatos szakpolitikai tevékenységek során éppúgy használható a jövőben, mint a kapcsolódó tudományos kutatások tekintetében.

DELI GERGELY

Az atomháború esélyei a mesterséges intelligencia korában

A 21. század biztonsági környezete a technikafejlődéssel jelentős változások előtt áll. Ennek az állam és jog területeire gyakorolt hatásai mellett számos politikai-társadalmi aspektusa is van. Fontos azonban a jelen kötetben tárgyaltak mellett azt is kiemelni, hogy ezek kapcsán úgy fest, a liberális békeelméletek egyre tarthatatlanabbá válnak a hadászati célú mesterséges intelligenciák elterjedésével. Ez a jelen tanulmány legfőbb következtetése, amely természetesen számos megszorítással érvényes. Egyrészt az érvelés csak azon liberális békeelméletekkel foglalkozik, amelyek kifejezetten Kant „Az örök békéhez" című munkájában lefektetett elvekre épülnek. Másrészt a számos különféle mesterséges intelligenciának (MI) nevezhető program közül csupán azon nem felügyelt mélytanulásra épülő rendszereket veszi számításba, amelyek bayesi elveken alapuló rétegekkel dolgoznak. Harmadrészt a szerző nem kíván állást foglalni a liberális békeelméletek és realista megfelelőik közti tudományos vitában. Csupán annyit állít, hogy az MI elterjedése negatív módon befolyásolja a liberális békeelméletek magyarázó erejét. Mindez persze azt is jelentheti, hogy egyre nagyobb lesz az esély a háborúra, ha nem veszik figyelembe a mesterséges intelligencia használatának elterjedése okozta változásokat a hadászattal összefüggő döntés-előkészítő folyamatokban. Negyedrészt nem úgy általában bármilyen háború kitörésének esélyeire fókuszál a tanulmány, hanem szűkebben, egy atomháború elméleti esélyeivel foglalkozik.

Ahhoz, hogy a bevezető mondatban megfogalmazott állítást alátámassza, a tanulmány az első lépésben azonosítja azokat a katonai területeket, ahol az MI alkalmazása befolyásolhatja egy nukleáris csapásmérésre vonatkozó döntéseket. Másodjára azonosítja a kanti felfogásra épülő liberális békeelméletek premisszáit. Az erre vonatkozó irodalom meglehetősen széles, azonban megmarad az állami szintű intézményi feltételek (pl. reprezentatív demokrácia) taglalásánál. Jelen tanulmány annyiban nyújt újat, hogy az „örök béke" rendszerszintű előfeltételeinek egyéni alapjait is igyekszik feltárni. Harmadrészt bemutatja, hogy gépi mélytanuló rendszerek „környezetfelismerése" mennyiben tér el az emberi megismeréstől, és hogy ennek a különbségnek milyen következményei vannak a nemzetközi békére. Mindezt természetesen szükségszerű az állam tágabb értelemben vett védelmi-biztonsági funkcióival is összekapcsolni a kortárs kihívások jobb megértése érdekében.

1. AZ MI SZEREPE A HÁBORÚ ÉS BÉKE KÉRDÉSÉBEN

A katonai célú MI-k elterjedése komoly következményekkel jár a nemzetközi stabilitás szempontjából. A szakirodalomban már számos figyelmeztető elemzés[1] született arról, miként befolyásolja negatívan az MI a nemzetközi stabilitást és vezethet el egy lehetséges katonai feszültség akaratlan[2] és hirtelen eszkalációjához.[3] Ha pontosan meg akarjuk érteni ennek okait, négy fő tényezőt érdemes közelebbről megvizsgálnunk. Az első fő ok, ami a háború esélyeit növeli a döntéseket befolyásoló események sűrűsödése, azaz hogy a technológiai fejlődés következtében sokkal több (emberi értelem számára gyakran feldolgozhatatlan mennyiségű) adat alapján kell sokkal rövidebb idő alatt döntéseket hozni.[4] A második tényező, ami az MI-vel összefüggésben destabilizálólag hathat, arra vonatkozik, hogy az MI tényleges és észlelt szerepe eltérő lehet. Ez a hadászati vonatkozású döntéshozatalokban, különösen az olyan érzékeny területeken, mint a nukleáris fegyverek bevetésének kérdése, kiemelten fontos lehet. Ugyanis a közeljövőben ezekben a helyzetekben az emberi részvétel, illetve kontroll nagy valószínűséggel erős marad. Ennek következtében az emberi, egyéni pszichés és morális tényezőket nem lehet kizárni az elemzésből. Az emberi közreműködés következtében a tényleges és az emberileg észlelt helyzetértékelések között nagy eltérések lehetnek. A harmadik veszélyforrást az képezi, hogy az MI felboríthatja a nukleáris nagyhatalmak

[1] Lásd a lényegesebbek közül Vincent Boulanin (szerk.): *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk, vol. I, Euro-Atlantic Perspectives*. Stockholm, SIPRI Publications, 2019; Edward Geist – Andrew J. Lohn: *How Might Artificial Intelligence Affect the Risk of Nuclear War?* Santa Monica, CA: RAND Corporation, 2018; Kareem Ayoub – Kenneth Payne: Strategy in the Age of Artificial Intelligence. *Journal of Strategic Studies,* 2016/5–6. szám, 793–819. o.; Technology for Global Security (T4GS) and the Center for Global Security Research (CGSR): AI and the Military: Forever Altering Strategic Stability. *T4GS Reports*, 2019 (https://www.tech4gs.org/); Jürgen Altmann – Frank Sauer: Autonomous Weapon Systems and Strategic Stability. *Survival* 2017/5. szám, 121–127. o.; James S. Johnson: Artificial Intelligence and Future Warfare: Implications for International Security. *Defense and Security Analysis,* 2019/2. szám, 147–169. o.

[2] Akaratlan eszkaláción azt a szituációt értem, amikor az egyik fél olyan lépést tesz, amelyről azt gondolja, hogy a másik fél részéről nem fog eszkalációhoz vezetni, mégis erre irányuló szándék nélkül, ilyenként értelmeződik. A szakirodalomból lásd Barry R. Posen: *Inadvertent Escalation: Conventional War and Nuclear Risks*. Ithaca, Cornell University Press, 1991; Forrest E. Morgan et al.: *Dangerous Thresholds: Managing Escalation in the 21st Century*. Santa Monica, CA: RAND Corporation, 2008; Lawrence Freedman: *Evolution of Nuclear Strategy.* London, Palgrave Macmillan, 2003, különösen a 14. fejezet.

[3] Lásd pl. James S. Johnson: Artificial Intelligence: A Threat to Strategic Stability. *Strategic Studies Quarterly*, 2020/1. szám, 16–39. o.

[4] Az időtényező fontosságát hangsúlyozza Hans M. Kristensen – Matthew McKinzie – Theodore A. Postol: How US Nuclear Force Modernization Is Undermining Strategic Stability: The Burst-Height Compensating Super-Fuze. *Bulletin of the Atomic Scientists*, 2017 (https://thebulletin.org/2017/03/how-us-nuclear-force-modernization-is-undermining-strategic-stability-the-burst-height-compensating-super-fuze/).

közötti status quót, és arra serkentheti az érintett államokat, hogy a technológiai fölény megszerzése vagy megtartása érdekében éles konfliktusokat vállaljanak fel.[5] Az MI-versenyfutás részben okkal azt a benyomást kelti, hogy az abban lemaradók örökre lemaradnak, a nyertesek pedig behozhatatlan előnyre tesznek szert. Ezzel összefüggésben a negyedik potenciális rizikó a katonai célú MI korai, nem biztonságos és nem előre kalkulálható használata, amely szintén jelentős eszkalációs faktort képez. Egyes elemzők szerint[6] veszély belátása vezette javarészt az USA Védelmi Minisztériumát (DOD), hogy a légierőnél állítsa le a „Tacit Rainbow" elnevezésű, pilóta nélküli radarromboló rakétafejlesztési programot. Hogy ez a negyedik veszélyforrás valóban jelentős, jól mutatja éppen az előbb említett fejlesztés esete. Ugyanis egyáltalán nem egyértelmű, hogy a program leállításának oka valóban stratégiai szintű belátás lett volna. A DOD 1991. június 24-én keletkezett, 91-102. számú jelentése[7] ugyanis számos szervezési hiányosságot és technikai nehézséget tárt fel. Akadozott a küldetéseket tervező szoftver előállítása, komoly logisztikai problémák merültek fel, illetve a szállítójárműnek kiszemelt F16-os vadászgépekkel való illeszkedési tesztek is csak évekkel később indulhattak volna meg. Azaz egyáltalán nem lehetünk biztosak abban, hogy kizárólag MI-specifikus hiányosságok esetén ugyanilyen döntés született volna.

Az imént röviden ismertetett négy tényezőt két fő csoportba oszthatjuk. Az első kettő, az idő rövidsége, illetve az emberi észlelés korlátai elsősorban egyéni kognitív szinten játszanak szerepet, míg a másik kettő, a versenyfutási kényszer és az elhamarkodott bevetés, pedig inkább állami, intézményi szintű kérdéseket vet fel. Azaz az MI elterjedésével összekapcsolható négy fő veszélyforrás vizsgálatakor egyaránt figyelemmel kell lennünk arra, hogy az új technológia miként befolyásolja az egyéni döntéshozatalt, illetve milyen kihatással van az állami döntéshozatali mechanizmusokra. A következő lépésben meg kell vizsgálnunk, hogy a liberális békeelméleteknek milyen intézményi és egyéni előfeltételei vannak, és hogy az imént röviden ismertetett veszélyek ezekkel milyen összefüggésben állnak, ha egyáltalán tételezhető közöttük valamiféle kölcsönhatás.

[5] Lásd Geist–Lohn: i. m. (2018); Ayoub–Payne: i. m. (2016), 799–819. o.

[6] Lásd Johnson: i. m. (2020), , 32. o. 12-es lábjegyzet.

[7] Memorandum for Under Secretary of Defense for Acquisition Assistant Secretary of the Navy (Financial Managment), Assistant Secretary of the Air Force (Financial Managment and Comptroller) (https://media.defense.gov/1991/Jun/24/2001714506/-1/-1/1/91-102.pdf).

2. A LIBERÁLIS BÉKEELMÉLETEK INTÉZMÉNYI ÉS EGYÉNI ELŐFELTÉTELEI

A kanti felfogásra épülő liberális békeelméletek szokásosan a nemzetközi stabilitás három fő oszlopát határozzák meg. Ezek a köztársasági képviseleti rendszer, az emberi jogok tiszteletben tartása, valamint a kölcsönös államközi függőségek. Ebben látják a Kant által szorgalmazott alkotmányos, nemzetközi és kozmopolita jogi normákat, amelyeknek egy megfelelő, hipotetikus békeszerződésnek tartalmaznia kell(ene). Egyesek hozzáteszik még, hogy a tartós béke eléréséhez egyszerre mindhárom feltételnek adottnak kell lennie.[8] Önmagában egyik feltétel sem elegendő, így még a demokratikus berendezkedés sem garantálja önmagában az államközi békét.[9] Az emberi jogok sem segítenek önmagukban, hiába ért bennük egyet a népesség túlnyomó része, ha ez a konszenzus nem képes ellenőrizhető és átlátható folyamatokon keresztül az állami szintű döntéshozatali mechanizmusok befolyásolására.[10] Végül semmi garancia nincs arra, hogy az államok közti gazdasági függőség önmagában ne tüzelné az imperialista tendenciákat, ha nem kapcsolódik hozzá kölcsönös bizalom és megbecsülés.[11] A köztársasági képviseleti rendszer azért lényeges, mert leginkább itt valósulhat meg az állam és polgárai, különösen az átlagos szavazók közötti olyan politikai viszony, amely megnehezíti, hogy a társadalom széles rétegeit érintően káros döntések szülessenek. Az egyéni, diktatórikus vagy monarchikus önkényt is a képviseleti, szavazati rendszer korlátozza a leginkább, és elősegíti az államot vezető elitek cseréjét, illetve körforgását. A széles képviseleti rendszerek hihetőbb és stabilabb nemzetközi elköteleződéseket képesek felvállalni, illetve létrehozni, és emiatt az ilyen demokráciák nehezebben keverednek háborúba.[12]

A képviseleti köztársaságok háborúinak a liberális értékek érvényesítéséért kell folyniuk. Ez természetesen nem visz közelebb a békéhez, mindaddig, amíg vannak

[8] Michael Doyle: Kant, Liberal Legacies, and Foreign Affairs. In Michael Brown – Sean Lynn-Jones – Steven E. Miller (szerk.): *Debating the Democratic Peace.* Cambridge: MIT Press, 1996., 27. o.; Michael Doyle: Liberalism and World Politics. *American Political Science Review*, 1986/4. szám,, 1162. o.; Michael Doyle: *Ways of War and Peace.* New York, Norton, 1997, 287. o.

[9] Lásd egyetértőleg John Mearsheimer: Back to the Future. *International Security,* 1990/1. szám 5–56. o.; Stephen Van Evera: Primed for Peace. *International Security*, 1990/1. szám, 58–107. o.

[10] John Mueller: *Retreat from Doomsday.* New York, Basic Books. 1989.

[11] Richard Cobden: *Political Writings of Richard Cobden.* London Ridgway, 1901; Eric Gartzke – Li Quan Li – Charles Boehmer: Investing in the Peace. *International Organization*, 2001/Spring, 391–438. o.

[12] James Fearon: Domestic Political Audiences and the Escalation of Political Disputes. *American Political Science Review*, 1994/3. szám, 577–592. o.; Kurt Gaubatz: Democratic States and Commitment in International Politics. *International Organization*, 1996/1. szám, 109–139. o.; Kenneth Schultz: Domestic Opposition and Signaling in International Crises. *American Political Science Review*, 1998/4. szám, 829–844. o.; Charles Lipson: *Reliable Partners.* Princeton, Princeton University Press, 2003.

nemliberális országok is. Azaz a demokratikus országok sem feltétlenül békések,[13] és akár a közelmúltból is számos példát találhatunk olyan fegyveres konfliktusokra, amelyet demokratikus országok vívtak nemliberális államokkal. Kant álláspontja szerint az ilyen háborúk jogtalanok, ugyanakkor követelményként állítja minden állam számára, hogy legyen részese a demokratikus államok minél nagyobb, lehetőleg az egész világra kiterjedő szövetségének, és így járuljon hozzá az örök béke megteremtéséhez. A „demokratikus" háborúk szempontjából kiemelkedő fontosságú a szabad sajtó és az átlátható kormányzás, hiszen csak ez biztosítja azt, hogy a közvélemény árnyalt és valós képet kapjon arról, milyen jogsértések történnek abban az országban, amelyik ellen államuk harcol, azaz pontosan milyen demokratikus értékért folynak a harci cselekmények. Csak így biztosítható a megfelel politikai kontroll a háború megindítása és folytatása tekintetében. A harmadik, kozmopolita tényező értelmében a szabad piacon, munkamegosztáson és szabadkereskedelmen alapuló gazdasági kapcsolatok hozzájárulnak ahhoz, hogy az államok sokat veszítsenek akkor, ha az ezekből folyó anyagi előnyök a háborús viszonyok következtében elvesznek vagy csökkennek. A liberális elméletek szerint ezek az értékek szoros összefüggést mutatnak a joguralommal, illetve tágabb értelemben véve a liberális berendezkedéssel. A másik szempont, amely a kölcsönös gazdasági függéssel összefüggésben felmerül a nemzetközi stabilitás szempontjából, az a tény, hogy a szabad piacot biztosító államokban számos fontos társadalmi döntés nem állami aktorok hatáskörébe kerül. Ez természetszerűleg magával hozza az esetleges konfliktusok esetén a békés, kompromisszumos megoldásra való törekvést, lévén ezek a szereplők jellemzően nem rendelkeznek hadászati képességekkel.

3. GÉPI KONTRA EMBERI „VILÁGMEGÉRTÉS"

A mesterségesintelligencia-kutatás egyik kiemelt területe manapság a gépi tanulás. Témánk szempontjából ez azért releváns, mert a szakértők között meglehetős egyetértés mutatkozik abban, hogy a gépi tanulás elengedhetetlen alkotóeleme lesz a jövőben megvalósuló, teljesen automatikus, katonai célú rendszereknek.[14] A gépi tanuló rendszerek olyan „önfejlesztő" algoritmusok, amelyek anélkül, hogy erre ki-

[13] Erről lásd Melvin Small – J. David Singer: The War Proneness of Democratic Regimes. *Jerusalem Journal of International Relations,* 1976/4. szám, 50–69. o.; Steve Chan: Mirror, Mirror on the Wall… Are the Freer Countries More Pacific. *Journal of Conflict Resolution*, 1984/4. szám, 617–648. o.; Eric Weede: Democracy and War Involvement. *Journal of Conflict Resolution*, 1984/4. szám, 649–664. o.

[14] Stuart Russell – Peter Norvig: *Artificial Intelligence: A Modern Approach.* Harlow, Pearson Education, 2014, 56. o.; Michael Horowitz – Paul Scharre – Alex Velez-Green – A Stable: *Nuclear Future? The Impact of Automation, Autonomy, and Artificial Intelligence.* Philadelphia, University of Pennsylvania, 2017.

fejezetten programozva lennének,[15] képesek bizonyos előrejelzések, illetve döntések meghozatalára. Ezt a látványos eredményt többnyire statisztikai alapon, az ún. tanító adatok modellezésével, azaz lényegében az adatokban fellelhető sajátosságok (mintázatok) feltárásával érik el.

A gépi tanulás egyik ígéretes területe a mélytanulás, amely a mély, azaz több rétegből álló, mesterséges neurális hálózatokon alapul. Ezek azért előnyösebbek más gépi tanuló algoritmusoknál, mert egyszerre képesek az adatokat a célnak leginkább megfelelő formátumra alakítani és azokat modellezni. Nehéz azonban esetükben eldönteni, hogy a hálózat melyik része végzi az adatok formázását és melyik a modellezést, ennek következtében a folyamatok utánkövetése vagy ellenőrzése aránytalan nehézségekkel járhat.

Egy mesterséges neurális háló egyszerű számítási egységekből, úgynevezett mesterséges neuronok hálózatából áll, melyek egymásnak küldött elektronikus vagy elektrokémikus jelekkel kommunikálnak. A rendszer általános „viselkedését" e kapcsolatok struktúrája és erőssége adja meg. A rendszer „tanítása" a neuronok közti kapcsolatok erősségének, az ún. súlymátrix értékeinek beállítása révén történik meg.

A csoportokba és rétegekbe rendezett neuronokat jellemzően három, funkcionálisan és strukturálisan jól elkülöníthető rétegbe, a bemeneti, a rejtett és a kimeneti rétegekbe szervezik. Ezeken belül a rétegeknek számos típusa létezik, ezek közül a négy legfontosabb az előrecsatolt *(fully connected, feedforward)*, a konvolúciós *(convolutional)*, a visszacsatolt *(recurrent)* és az autoenkóder *(autoencoder)* egységek. A kimenet alapvetően három tényezőtől függ: a bemenet, a neuronok átviteli jellemzői és a súlymátrix (azaz a neuronok közti kapcsolatok erősségének, súlyának rendszere) együttesen alakítják.

A neurális hálók bemeneti és kimeneti neuronjainak száma a megoldani kívánt feladathoz igazodik. A belső rétegek száma és az őket alkotó neuronok mennyisége már szabadabban alakítható, azonban a túl kevés neuron kevés minta tárolását teszi lehetővé, ami hátráltathatja a betanulást. Túl sok neuron esetén pedig a háló betanul ugyan, de a korábban nem látott bemeneti jelekre rosszul válaszol, a feltárt mintázatok nem lesznek eléggé absztraktak, és a rendszer adatbázisszerűen fog működni. Ezeket a hibákat nevezi a szakirodalom *under-* és *overfitting*nek.

A gépi tanulás folyamata lehet felügyelt vagy felügyelet nélküli. Az előző esetében a tanulási adatokat előzetesen felcímkézik (tagged), az utóbbinál a rendszer maga „keres" mintázatokat az adattömegben. A bayesi típusú neurális hálózatok (BNH) a

[15] E fordulat eredetéhez lásd A. L. Samuel: Some studies in machine learning using the game of checkers. *IBM Journal of Research and Development*, 1959/3. szám, 210–229. o., J. R. Koza – F. H. Bennett – D. Andre – M. A. Keane: Automated Design of Both the Topology and Sizing of Analog Electrical Circuits Using Genetic Programming. In J. S. Gero – F. Sudweeks (szerk.): *Artificial Intelligence in Design*. Dordrecht, Springer, 1996.

felügyelet nélküli mélytanulás egyik lehetséges válfaját alkotják. A Bayes-tétel alapján dolgozó rétegeket *(probabilistic layers)* alkalmaznak, amelyek hozzásegítenek a fenti hibák elhárításához a belső rétegek és neuronok optimális számának meghatározásán keresztül, illetve a kimeneti eredmények előrejelzésében is szerepet játszhatnak.

Jelen tanulmány keretei között azért a bayesi típusú neurális hálózatokra (a továbbiakban: BNH) esett a választás, mert ezek működési elve hasonlatos az emberi megismeréshez. Mindkettő az észlelt adatokban „természetesen" előforduló szabályszerűségeket keres, és saját működését bizonyos szűrőkön keresztül optimalizálja. Amíg a BNH statisztikai alapon egyszerűsíti a saját folyamatait, az emberi megismerés ökölszabályokhoz és korábbról adott szokásokhoz igazodik. Így egyik működése sem szigorúan determinált. Végül a belső működés mindkét esetben kevéssé átlátható és utánkövethető.

Hogyan illeszthető most már e két megismerési metódus, az emberi és BNH-n alapuló a kanti etikába?

A kanti ismeretelmélet szerint az emberi megismerés két forrásból táplálkozik. Az egyik az érzéki észlelés (sinnliche Anschauung), a másik pedig az értelem (Verstand). Az előzőnek a fizikai tárgyak, az utóbbinak a fogalmak a tárgyai. Ez a kettősség teszi szükségszerűvé az ember szempontjából a lehetségesség és a valóság dualitását. Emiatt egyrészt amit lehetségesként képesek vagyunk elgondolni, nem biztos, hogy létezik. Ez egy „kemény" következmény. Ezen az alapon *ad extremum* egy objektív és abszolút létezőt (Istent) is lehetségesként tudjuk elképzelni, sőt egy ilyen létezőt Kant szerint szükségszerűen a fenti attribútumokkal kell elképzelnünk. Ez azonban az előző logikai viszonyhoz képest egy „puha" következmény.

A kanti megismerés folyamata egy lineáris modell segítségével is leírható. A bemeneti oldalt a fizikai objektumokra vonatkozó észlelet jelenti. Ez a BNH esetében a bemeneti réteget elérő adathalmaznak felel meg, amelyet a rendszer számára szenzorok vagy egyéb metódusú bevitel tesz hozzáférhetővé. A modell következő lépcsőfokát az értelem adja, amely az érzékileg észlelttel olyan viszonyban áll, hogy szükségszerűen fel kell ismernie, hogy az érzékelt dolog létezésének csupán lehetségességét és nem a valóságát képes biztosítani. Ennek a felismerésnek az okáról bizonyossággal nem állítható, hogy magában a dologban rejlene. Ez akár így is lehet, de nem szükségszerűen van így, és inkább az emberi megismerés speciális adottságainak köszönhető. Az értelem eszközei ugyanis nem az érzéki képek, hanem a fogalmak, emiatt az értelem az általánostól halad a különös felé a megismerés folyamatában. Ebből a szempontból az értelem közelebb áll az észhez (Vernunft), mint az érzékeléshez, hiszen az ész eszközei az elvek, amelyek a fogalmak tartalmai és formai jellemzőit elsősorban meghatározzák. Ez még akkor is így van, ha a fogalmaktól az elvekig tartó út teljesen nem bejárható. Fogalmainkkal szükségszerűen nem tudunk bizonyos elveket teljes mértékben leírni, vagyis valóságosságukat kétséget kizáró módon belátni. Az értelem és az általa használt fogalmak korlátai ugyan szükség-

szerűen okozzák egy abszolút létező lehetségesként történő feltevését, de nem tudják annak valóságosságát bizonyítani. Emiatt az ész nem képes objektív, szintetikus, illetve konstitutív értékítéletek megalkotására, csupán regulatív elvek felismerésére. Ez a BNH esetében is fennáll. Hiszen a BNH által felismert mintázatokról nem tudható bizonyosan, hogy azok valóban konstitutív erejűek-e. Nyomós okunk van feltételezni, hogy ezek is egyszerűen a puszta regularitás szintjén maradnak, a BNH esetében konkrétan a statisztikai valószínűség regularitásán nyugszanak. Azaz ebben a vonatkozásban az emberi és mélytanuláson alapuló megismerés megegyezik. Nem szabad elfelejtkeznünk arról a tényezőről sem, hogy, mint már fentebb láttuk, Kant lényegében feltette egy abszolút, objektív létező létének lehetőségét. A kvantumfizikai kutatások azonban abba az irányba mutatnak, hogy el kell szakadnunk egy objektíve, azaz determinisztikusan adott világ eshetőségétől, vagy legalábbis bele kell nyugodnunk, hogy ha van is ilyen, azaz emberi megismerés elől természetszerűleg rejtve marad. A mai fizika álláspontja szerint a világ nem determinisztikus, csupán sztochisztikus. Mindez azonban nem jelenti szükségszerűen azt, hogy a világ eshetőleges minéműsége és a mélytanulás eshetőlegessége ugyanolyan vagy akár csak hasonló „természetű" eshetőlegesség lenne. Azaz csupán a BNH sztochisztikus jellege önmagában nem garancia arra, hogy a valószínűségi elveken alapuló univerzumot jobban megértjük általa.

Ha az értelmünk szemléleti jellegű lenne, azaz ha eszközei nem fogalmak, hanem közvetlenül a dolgok észleletei lennének, akkor az értelem nem egyszerűen a lehetségest, hanem magát a valóságost ismerné meg. Továbbá nem léteznének sem a nekünk valamit tárgyként való tételezettség nélkül adó észleleti képek, sem a dolgoknak csupán a lehetségességét (és nem valóságosságát) megállapítani képes fogalmak. Kant felfogásában a lehetséges és valós dolgok megkülönböztetése az emberi értelemre jellemző, szubjektív adottság. Nem zárja azonban ki, hogy más megismerőre is jellemző lehet ez a dualitás. És valóban, a BNH esetében is megtalálhatjuk ezt a kettősséget, még ha egészen más formában is. Ugyanis a BNH-ban nincs analógiája az értelemnek. Az MI nem gondolkozik fogalmakban, a kanti lineáris episztemológia megbicsaklik, és a sorban a fizikai észlelés után közvetlen az elvek, azaz az adatokban felismert mintázatok következnek. A BNH-nak az emberhez hasonlatosan van észlelése, és van kanti értelemben vett esze (Vernunft) is, azonban – az embertől eltérően – nincs értelme (Verstand). A BNH nem fogalmi alapon közelíti meg az elveket, azaz a valóságban adott törvényszerűségeket, hanem észleleti alapon. Mégsem mondható el róla, hogy észlelése alapján szükségszerűen a valósághoz jut el. Hiszen ugyan az általa felismert mintázatok a rendszer szempontjából bizonyosan léteznek ugyan, de nem feltétlenül biztos, hogy csak ezek a mintázatok léteznek, illetve hogy a feltárt mintázatok azok a mintázatok-e, amelyeket valóban érdemes megismerni, azaz nem garantált, hogy a feltárt mintázatok adják a valóság lényegi mintázatait, már ha egyáltalán létezik ilyen. Hiszen a BNH nem determinisztikus alapon funkcionál, másrészt számítási kapacitásai is végesek. Így a BNH által felismert mintázat

vagy törvényszerűség valóban benne van az észlelt világban, és ennyiben valóságos, de nem mondható bizonyosan, hogy „igaz" is. A BNH által megállapított mintázat vagy kanti értelemben elv valódisága nem bizonyos, csupán valószínűségi. A Bayes-tételen alapuló kimeneti szűrő optimalizálja a közbenső, „tanuló" rétegek számát, és ennek köszönhetően a rendszer eléggé elvont eredményt ad, azaz az output nem tapad majd túlságosan az adatokhoz adatbázisszerűen, de nem is nagyolja el tendenciaszerűen a finomabb mintázatokat. Azaz megóvja a mélytanuló rendszert mind az under-, mind az overfitting veszélyétől. Azt azonban nem garantálhatja, hogy az így feltárt mintázat az adatokban rejlő törvényszerűséget hiánytalan pontossággal leképezi, vagy hogy valóban a „valódi" mintázatokat tárja fel.

A lehetségesség és valódiság emberi megismerésre jellemző dualitása nagymértékben különbözik a BHN megismerésének dualitásától. Mivel a BHN-ben nincs értelmi, azaz fogalmi szint, maga a rendszer önmagában az érzékileg adottból azonnal eljut az elvileg adotthoz, anélkül hogy eközben a lehetségesként adott felmerülne benne. A lehetőség megjelenik ugyan a rendszerben, hiszen a bayesi réteg alkalmas arra, hogy egy bizonyos valószínűséggel előrejelezze, milyen adat lesz az új adat. Ez a lehetségesség azonban a mintázatokhoz képest, azaz a korábban érzékelt adatokhoz képest, érzéki-elvi szinteken jelentkezik a BHN-ben, és nem az értelmi szinten, mint az emberi megismerés esetében. Ez a különbség az oka annak, hogy a BHN, az emberi megismeréstől eltérően, nem teszi fel szükségszerűen egy ősok (Urgrund) létét. Az emberi megismerés az abszolút létező létét „puha" Sollenként tételezi, hiszen csak a maga szubjektív megismerési adottságaiból képes azt levezetni. Isten létét az ember az észbeli okozatiságra (Vernunftkausalität) alapozza, azonban a maga totalitásában azt értelmileg felfogni sohasem lesz képes. Ennek oka Kant szerint az emberi megismerés érzéki jellegéből fakad, azaz abból, hogy nem magukat a dolgokat ismerjük meg, csak a dolgok érzéki megjelenését. Azaz az emberi megismerésben a „puha" Sollennel szemben egy „puha" Sein áll. A BHN Sollenje keményebb az emberinél. Ennek oka, hogy a felismert mintázat avagy törvény ténylegesen ottlévőként tételeződik, mert az onnan hiányzó értelem nem bontja szükségszerűen lehetségesre és valóságosra a megismert világot. A BHN Seinja az emberihez hasonlóan puha, a használt szenzorok milyenségétől és minőségétől függ.

Mivel a BHN esetében nincs meg az érzéki és az értelmi megismerés kettőssége, ezért az általa megismert tárgyak „vannak" (sind), illetve léteznek (existieren). Ennek következtében annak feltevése, hogy lehetségesek az egyébként nem létező dolgok is, azaz hogy ilyenek akár véletlenül, akár ettől megkülönböztetendően szükségszerűen is létezhetnek (mint mondjuk Isten), egy BHN megismerési folyamatában nem merülhet fel.

A BNH-ban az értelem, a fogalmi megismerés hiányában nem beszélhetünk az észlelt dolgok tárgyként való felismeréséről sem. A BNH nem áll mintegy megismerőként alany-tárgyi relációban az észlelt dolgokkal. Az alanyiság ezen hiánya miatt kétséges jogalanyisága is. Nem szükségszerű azonban, hogy ez mindig így marad.

A technológiaváltozások magukkal hozhatják olyan többszintű rendszerek alkalmazását, amelyek a saját megismerési folyamataikra reflektálnak. Ha ez megtörténik, akkor létrejöhet mesterséges kapcsolat a megismerés folyamata és a megismerés tárgya között, amennyiben maga a megismerés folyamata lesz a megismerés tárgya is. Ez még ekkor sem jelenti majd feltétlenül azt, hogy az ilyen rendszerek alanyiságát el kellene fogadnunk, hiszen továbbra is érvelhetünk úgy, hogy a jogalanyiság eszszenciális lényegét nem az alany-tárgyi viszony meglétéhez, hanem a fogalmi gondolkodáshoz kötjük. Ekkor a jogalanyiságra vonatkozó kérdés megválaszolása azon fog múlni, hogy a többszintű önreflektív öntanuló algoritmusok működését fogalmi működésnek tekinthetjük-e.

Mivel, ahogy arról már szó volt, az emberi ész elvi szinten egy ősok létét szükségszerűen fel kell, hogy tegye, ezért a gyakorlati szinten a maga feltétlen okozatiságát, azaz szabadságát is tételeznie kell. Kant szerint a gyakorlati megismerés szubjektív adottságai következtében az embernek az erkölcsi törvényeket parancsokként kell elképzelnie. Emiatt az egyébként szükségszerűen létező törvény szerinti cselekvés csupán lehetőség az ember számára. Az ész az erkölcsi törvény szükségszerűségét nem Seinként, hanem csupán Sein-Sollenként fejezi ki. A BNH számára az általa felismert mintázat, azaz az adathalmazban benne lévő törvény Seinként jelentkezik. Ebből fakad, hogy az MI számára a Sein-Sollen nem az elv, nem a törvény szintjén, hanem az érzéki szinten érvényesül. A BHN nem a mintázatról észleli annak szükségszerűségét, hanem a következő bemeneti adat mibenlétéről, és azt is csak valószínűségi alapon. Maga a mintázat a bemeneti adat milyenségétől függ a Bayes-tételnek megfelelően.

A BHN-ben is van azonban szabadság! Ez azért van, mert a BHN-ben is értelmezhető az érzéki és az elvi szint. Amiatt, hogy ez a kettő a BHN esetében sem kapcsolódik össze okozati, determinisztikus szükségszerűséggel, adódik a szabadság léte. Azaz a BHN sem kötött feltétlen módon abban, hogy milyen mintázatot, törvényszerűséget fedez fel. Elképzelhető ugyanis, hogy két azonos felépítésű BHN ugyanazon adathalmazból (még ha kismértékben is, de mégis) eltérő törvényszerűségeket tár fel. Amíg a szabadságot az emberi esetben az értelem korlátozottsága (érzéki kötöttsége, és az, hogy fogalmaival nem képes maradéktalanul megközelíteni a törvényeket) okozza, addig a BHN esetében a szabadság az értelem teljes hiányából fakad. A két szabadság között azonban lényeges különbség van. Az ember esetében a szabadságot az ész tételezi, azért, mert az ész szükségszerűen az általánostól halad a különös felé. Az értelem szintjén pedig azzal szembesül, hogy a különöst csak lehetségesként képes tételezni, így az általános elv és a konkrét, különös cselekvés között szükségszerűen tátong egy fogalmi űr, a szabadság terepe. Ezért az ember esetében a szabadság „megélt", reflektált szabadság, hiszen az értelem a maga sajátosságainak köszönhetően szükségszerűen szembesül a maga korlátaival. A BHN megismerési folyamata ezzel szemben a különöstől halad az általános felé. És ezen az úton a szabadság ugyan megtörténik, de nem tételeződik. A BHN-nek nincs ér-

telme, pláne nincs olyan értelme, amely a lehetségesség-valódiság dualitására szükségszerűen reflektálna. Ezért a BHN nem „érzi" magát szabadnak.

Másrészről az ész, mivel az általánostól halad a különös felé, egy általános törvény nélkül, amely alá a különös adatok szubszumálhatná, nem lenne képes sem a különösben rejlő célszerűséget fellelni, sem értékítéleteket alkotni. Mivel azonban a különös, az általánostól tekintve mindig valamilyen véletlenszerűséget rejt magában, de az ész mégis egységes törvényszerűséget követel meg (ezt a törvényszerűséget hívja Kant a véletlen célszerűség törvényszerűségének), ezért a tárgyakról alkotott fogalmakon keresztül az általános törvényekből nem képes *a priori* a különös törvényeket levezetni. Mindez azt jelenti, hogy az értelem a fogalmai révén nem képes arra, hogy a bizonytalan érzéki észlelés nélkül az általa szükségszerűen felismert általános elvekből különös törvényeket alkosson. Azaz a természeti célszerűség ugyan szükségszerűen felismert fogalom lesz, ez a szükségszerűség azonban nem a természet dolgaiban rejlik, hanem az emberi megismerés sajátosságaiban. Ez egy, az ész által felismert szubjektív (azaz emberi okokon nyugvó) törvényszerűség, amely azonban éppolyan szükségszerűen érvényes Kant szerint, mintha objektív törvényszerűség volna.

Mivel a BHN-ben a törvény nem az ész felismerése (mivel a BHN-ben nincs is ész), és mivel megismerése nem az általánostól halad a különös felé, hanem éppen fordítva, ezért a feltárt mintázatok mint törvények semmiképpen sem lehetnek a priori törvények, csakis a posterioriak. Az eredmény tehát ugyanaz: sem az ember, sem a BHN nem képes a tapasztalattól függetlenül különös törvényeket alkotni. A BHN más azonban annyiban, hogy az általa feltárt törvényszerűségek (azaz mintázatok) mindig különösek, sohasem általánosak. Ezek a BHN felépítéséből adódó szubjektív törvényszerűségek, mégis, hasonlóan az emberi megismerés esetéhez, objektív szükségszerűség erejével hatnak. Lényeges azonban, hogy mivel a BHN a különöstől halad az általános felé, számára a törvényszerűség általános vagy különös jellege között nincs különbség. Minden törvényszerűség ugyanolyan mértékben adott (ist) a BHN számára, és ugyanolyan episztemológiai távolságra van az érzékileg adott tárgyi valóságtól.

A lényeg mindebből az, hogy a BHN esetében a törvény (a mintázat) a valószínűség törvényszerűségeinek közvetlenségével az érzékileg adottból ered, míg az ember a különös törvényt az elvekből vezeti le a szükségszerű lehetségesség keretében az értelem érzékileg kötött fogalmai segítségével.

***

A fenti fejtegetések során először azt a négy rizikófaktort azonosítottuk, amelyek révén az MI katonai célú használata megnövelheti egy esetleges nukleáris konfliktus eszkalációjának esélyét. Azt találtuk, hogy az MI elterjedése mind az egyéni döntéshozatalt, mind pedig az állami, akár demokratikus döntéshozatali folyamatokat úgy befolyásolhatja, hogy azok inkább a destabilizáló tényezőket erősíti. Ezt követően

azonosítottuk a kanti alapú liberális békeelméletek intézményi és egyéni előfeltételeit. A vonatkozó irodalom áttekintése során azt találtuk, hogy míg az elsővel, azaz a béke intézményi előfeltételeivel igen bőséges irodalom foglalkozik, ritka az olyan elemzés, amely a liberális teóriák egyéni, személyi döntéshozói szintjére fókuszálna. Tanulmányunk ebben a vonatkozásban is szolgált tudományos nóvumokkal. A rizikófaktorok és a béke előfeltételeinek összevetése azt az eredményt hozta, hogy az MI az azonosított veszélyeken keresztül mind az egyéni, mind pedig intézményi szinten gyengíti azon előfeltételek fennmaradásának, illetve előállításának esélyét, amelyek a vonatkozó elméletek szerint a nemzetközi béke és stabilitás szempontjából elsőrangú fontosságúak.

Így megerősítést nyert a kutatás hipotézise, azaz belátható, hogy a liberális békeelméletek magyarázó ereje az MI katonai célú elterjedésével csökken. Ez pedig azt a veszélyt is magában hordozza, hogy az ilyen elméletekre alapozott katonai, illetve külpolitikai döntéshozatal egyre kevésbé lesz képes értelmezni a felmerülő kihívásokat, és azokra adekvát válaszokat megfogalmazni. Azaz az ilyen típusú elméletekhez való ragaszkodás maga is rizikófaktorrá válik, és súlyosbítja azt a problémát, amely az MI-k sajátosságai miatt amúgy is fennáll.

SMUK PÉTER

A politikai diskurzus és torzulásai: szabad deliberáció vs. befolyásolás

Alkotmánytani megközelítésben demokratikus eljárások érdemi előfeltételének tarthatjuk, hogy a politikai közösség (mint a közhatalom forrása) tagjainak érdemi részvételi jogai biztosítottak legyenek egy szabad és sokszínű kommunikációs mezőben. A kommunikációs jogok együttese „teszi lehetővé az egyén megalapozott részvételét a társadalmi és politikai folyamatokban… az egyéni véleménynyilvánítás, a saját törvényei szerint kialakuló közvélemény, és ezekkel kölcsönhatásban a minél szélesebb tájékozottságra épülő egyéni véleményalkotás lehetősége az, ami alkotmányos védelmet élvez", és egyben az alkotmány „a szabad kommunikációt – az egyéni magatartást és a társadalmi folyamatot – biztosítja, s nem annak tartalmára vonatkozik a szabad véleménynyilvánítás alapjoga. Ebben a processzusban helye van minden véleménynek, jónak és károsnak, kellemesnek és sértőnek egyaránt, különösen azért, mert maga a vélemény minősítése is e folyamat terméke."[1] A saját törvényei szerint alakuló közvélemény vagy „vélemények piaca" a kibertér 21. századi, innovatív eszközeinek és ezek hatalmi érdekek szolgálatába állításának fényében talán naiv elképzelésnek tűnik. E kötet a téma állami és jogi, politikai-társadalmi, valamint tág értelemben vett védelmi védelmi-biztonsági vonatkozásait is áttekinti, melyek mellett dolgozatomban szükségesnek tartom annak áttekintését, hogy a demokrácia védelme érdekében miként jellemezhető ezen kommunikációs mező, az annak eltorzítására irányuló törekvések, valamint az ezekkel „szembeni" eszközrendszer.

1. A POLITIKAI DISKURZUSOK DEMOKRATIKUS JELENTŐSÉGÉRŐL ÉS ALKOTMÁNYOS GARANCIÁIRÓL

A közvetlen hatalomgyakorlás, a népszavazás kivételes alkalmai és a képviselőkre való hatalomátruházás során is a polgár felelősségteljes, tudatos döntésében bízhatunk. Ezt a felelősségteljes közreműködést az alapozhatja meg, ha információk birtokában van a döntés tárgyát illetően (a tágabb értelemben vett kormányzat tevékenységéről, a közügyekről). Az információk megszerzése nem csupán úgy lehet-

[1] 30/1992. (V. 26.) AB határozat.

séges, ha az állami szervek a működésükkel kapcsolatos adatokat kiadják a polgárok számára. Ezen információtömeg ugyanis feldolgozhatatlan mennyiségű és minőségű, rendezetlen, és így feldolgozásra szorul. A politikai rendszer teljesítményének értékeléséhez csak „fogyasztásra alkalmas" állapotban elérhető információk segítenek hozzá. A közérdeklődésre számot tartó adatok ilyen feldolgozását a politikai közösség tagjai részére a közvélemény diskurzusa végzi el.

A demokratikus politikai diskurzus a közvélemény nehezen definiálható fogalmához köthető. A Habermas által „nyilvános okoskodásnak" nevezett jelenség folyamatként fogható fel, amelynek több (a lehető legtöbb) aktív szereplője van. A modern, általánosan felfogott közvélemény a sajtó és a média tevékenységében nyilvánul meg, de csatlakoznak hozzá különféle fórumok és felületek is („okoskodó" körök: pl. egyesületek, klubok; véleményformáló intézmények: pl. színházak; stb.).[2]

Számunkra jelen elemzés felépítéséhez a szereplők tág körének rögzítése mellett az is szükséges, hogy a demokratikus közvélemény és politikai diskurzus létrejöttének és működésének alkotmányos garanciáit felvázoljuk. Ezek egy központi érték, a kommunikációs alapjogok érvényesülése köré csoportosíthatóak. A deliberatív politikai viták és demokratikus eljárások fogalmi eleme, előfeltétele és garanciája ugyanis a szabad kommunikáció.

A szabad kommunikáció alkotmányos garanciái körében a klasszikus alapállás az állam beavatkozástól való tartózkodása, praktikusan a vélemények elhallgattatásának, az előzetes cenzúra, illetve az adminisztratív hátrányok utólagos, megtorló alkalmazásának tilalma. Ez az álláspont semmit sem veszített érvényességéből, azonban a demokratikus véleményformálás, politikai diskurzus ezen az alapon kevés támogatást kap. Erről a magyar Alkotmánybíróság tömör és pontos leírást adott a már említett, korai határozatában: „Az egyéni véleménynyilvánítási szabadság szubjektív joga mellett tehát az Alkotmány 61. §-ából következik a demokratikus közvélemény kialakulása feltételeinek és működése fenntartásának biztosítására irányuló állami kötelezettség. A szabad véleménynyilvánításhoz való jog objektív, intézményes oldala nemcsak a sajtószabadságra, oktatási szabadságra stb. vonatkozik, hanem az intézményrendszernek arra az oldalára is, amely a véleménynyilvánítási szabadságot általánosságban a többi védett érték közé illeszti. Ezért a véleménynyilvánítási szabadság alkotmányos határait úgy kell meghatároznia, hogy azok a véleményt nyilvánító személy alanyi joga mellett a közvélemény kialakulásának, illetve szabad alakításának a demokrácia szempontjából nélkülözhetetlen érdekét is figyelembe vegyék."[3]

[2] A közvélemény államjogi problematikájához és szociológiai tisztázási kísérletéhez lásd Jürgen Habermas: *A társadalmi nyilvánosság szerkezetváltozása*. Budapest, Osiris, 1999, 332–349. o. Az ehhez is kapcsolódó, jelen tanulmányra is érvényes kutatói alapálláshoz (Habermasra utalóan) lásd Bajomi-Lázár Péter – Sükösd Miklós: Médiapolitikai trendek Kelet-Közép-Európában 1989–2008. *Politikatudományi Szemle*, 2009/1. szám, 143–144. o.

[3] 30/1992. (V. 26.) AB határozat.

Az állam intézményvédelmi szerepének előtérbe kerülése több, legújabb kori fejlemény miatt következett be. A kommunikációs folyamatok, a „társadalmi nyilvánosság szerkezete" merőben átalakult, nemhogy a polgári forradalmak korától eltelt évszázadokban, de az elmúlt tíz-húsz évben is radikális újdonságok jelentek meg. Az egyéni autonómia védelme helyett-mellett a közvélemény információhoz jutása került előtérbe: kiemelt szabályozási tárgy lett az audiovizuális kommunikáció területe, különös tekintettel a pluralizmusra és a közérdekű tartalmaknak közvetlenül a polgárhoz való eljuttatására. A digitális eszközök, különösen az internet pedig egyrészt a közvélemény „szétesését", decentralizációját hozták, másrészt a nemzeti szabályozó eszközök eltörpülését eredményezték a globális kihívásokkal szemben.[4]

A szólásszabadság demokratikus igazolása szerint a különféle véleményeket azért lehet elmondani, mert azok „relevánsak", akár okos, akár észszerűtlen tartalmúak, hiszen a polgárok önkormányzását segítik elő (Meiklejohn); illetve, más nézet szerint az egyének közéletben való részvételét biztosítják, azáltal pedig az egyéni képességek kiteljesítéséhez járulnak hozzá (Robert Post).[5] A véleményszabadság tehát eszköz-érték is, amely a népszuverenitás elvét (is) szolgálja. A demokrácia és az alkotmányos jogok esetleges ütközése a modern jogállamokban nagyrészt az utóbbiak javára dőlt el, tehát a demokratikus alapjog-korlátozások problematikája[6] nagyrészt elvi, hipotetikus kérdésfeltevésnek tűnhet. Két előfeltevés tisztázandó mégis ezen a helyen.

A deliberatív demokráciafelfogásban a politikai diskurzusok célzatosak, az „okoskodó közönség" nem egyszerűen beszélget egymással, hanem érvelnek, egymást igyekeznek meggyőzni, az üdvös végeredmény pedig az igazság megtalálása, de legalább a megegyezés, amely az érvek alapján jöhet létre. Ezt a célt – ennek a célnak az elérésére irányuló szándékokat – azonban a mindennapi tapasztalat csak kevéssé igazolja vissza. Úgy kell eljárnunk, hogy a lehető legtöbb véleményt a demokratikus diskurzus részének tekintünk,[7] ugyanis adott pillanatban nem mindig megítélhető, hogy azok mennyiben járultak hozzá az igazság vagy a megegyezés kereséséhez. Így a *prima facie* káros vagy terméketlen vélemények védelmét is a deliberatív felfogáshoz kapcsolhatjuk.[8]

[4] Joan Barata: The different concepts of free expression and its link with democracy, the public sphere and other concepts. In Monroe E. Price – Stefaan G. Verhulst – Libby Morgan (szerk.): *Routledge Handbook of Media Law.* London/New York, Routledge, 2013, 125. o.

[5] Koltay András: A médiaszabályozás elmélete. In Koltay András – Nyakas Levente (szerk.): *Magyar és európai médiajog.* Budapest, Complex, 2012, 90. o.; Sajó András: *A szólásszabadság kézikönyve.* Budapest, KJK-Kerszöv, 2005, 22–25. o.

[6] Koltay: i. m. (2012), 91. o.

[7] Lásd még Robert Post: Participatory Democracy and Free Speech. *Virginia Law Review*, 2011/3. szám, 477–489. o.

[8] Győrfi Tamás: 2. § [Alkotmányos alapelvek; ellenállási jog.] In Jakab András (szerk.): *Az Alkotmány kommentárja.* Budapest, Századvég, 2009, 151–152. o.

Másrészt a politikai diskurzust folyamatként fogjuk fel, már csak az előbbi megállapítás alapján is: nem a vélemények ütköztetésének egy adott pillanata határozza meg elsősorban a hatalomgyakorlást és a demokratikus részvételt, hanem a közügyekről folytatott vita és a választásokon való folyamatos részvétel. Luhmann legitimitáselmélete az uralmi szférában a legitimitás keletkezését eljárásokhoz köti. Az eljárások, mint a törvényhozás, jogalkalmazói döntések, népszavazás, de a korporációk eljárásai is, valamiféle általánosított készséget alakítanak ki, hogy a politikai közösség tagjai „tartalmilag meg nem határozott döntéseket egy bizonyos toleranciahatáron belül elfogadjanak". Ez az általános elfogadási attitűd olyan diskurzusokat feltételez, amelyek során megvitathatóak a közügyek, azokban külön-külön álláspontokat tudunk elfoglalni, meg tudjuk egymást győzni (Habermas).[9] Luhmann és Habermas processzuális legitimitáselméleteit mélyebben nem elemezve azt kell rögzítenünk, hogy a vélemény- és sajtószabadság, valamint annak infrastruktúrája ezen eljárásoknak természetes előfeltételeként, közegeként működik. Mind a társadalmi-állami eljárások, mind pedig a kritikai – akár deliberatív, akár más – viták számára. Ezeknek a politikai diskurzusok biztosításával kapcsolatos intézményi garanciáknak a sorában főként a parlamentek nyilvános működése, a választási kampányok, az információszabadság alapintézményei, valamint a – klasszikus és ún. „új" – média piaca és a médiatartalmak pluralizmusa vizsgálandóak.[10]

A politikai diskurzusok színvonalát és sikerét is meghatározza, hogy a résztvevők számára az adott ügyben és általában a közügyekben álljanak rendelkezésre a releváns információk. Ezen információk beszerzésének lehetősége, szándéka, azok feldolgozása azonban korántsem egyértelmű vagy általános. A racionális viták és eredményük, a racionális megállapodás így hipotetikus, sőt többen, a deliberatív elméletek kritikusai, a diskurzus bukásáról *(„theory of discourse failure")* beszélnek. Szerintük a választópolgárok racionális hozzáállása az, hogy nem érdekli őket a szavazás eredménye, hiszen nem érzik, hogy azt szavazatuk befolyásolni tudná. Ezért nem költenek sokat sem az információszerzésre, sem a még költségesebb deliberációban való részvételre. A többségi demokráciában a politikusok – akik a maguk egyéni céljainak megfelelő redisztributív hatalmi döntések elérésére törekednek – hamar rájönnek a választók érdektelenségére és tudatlanságára, ezért hamis és önérdeküket szolgáló adatokat, értékeket és elméleteket propagálnak. Ilyen körülmények között a diszkurzív elmélet összeomlik.[11]

[9] Zsidai Ágnes: Legitimitás és legitimáció. In Takács Péter (szerk.): *Államelmélet.* Miskolc, Bíbor, 1997, 338–341. o.

[10] A média politikai folyamatokban betöltött szerepéről és átpolitizálódásáról, valamint további olvasmányokhoz a hazai szakirodalomból lásd Bajomi-Lázár Péter: A politika mediatizálódása és a média politizálódása. *Médiakutató*, 2005/ősz.

[11] Guido Pincione – Fernando Tesón: *Rational Choice and Democratic Deliberation: A Theory of Discourse Failure.* Cambridge University Press, 2006; kritikai áttekintését adja recenziójában Gerry Mackie: Reviewed. *Notre Dame Philosophical Reviews*, 2007. (http://ndpr.nd.edu/news/23149/?id=11143)

2. A SZABAD INTERNET ROMANTIKÁJA

Az új típusú médiaszabályozások egyik fő jellemzője, hogy kiterjesztik hatályukat a világhálóra, mert felismerik, az internet egy olyan platformmá vált, amely nemcsak alkalmas a hagyományos módon sugárzott műsorok új felületen való megjelenítésére, hanem új típusú kommunikációs szolgáltatásokat és formákat is lehetővé tesz – amellyel pedig sikerrel hívta ki a fogyasztók körében általánosan legnépszerűbb televízió vezető pozícióját. A médiaszabályozáson túl egyéb jogágak hatása is megállapítható az internetre – bár a kibertér teljes szabályozatlansága a demokrácia modern, romantikus felfogásában élénken jelen van.[12]

A demokratikus eljárások átalakulására is lehet hivatkozni, amikor azt látjuk, hogy a korábbi „egyirányú" média fogyasztásával ellentétben az internet aktivizálja és mobilizálja az embereket, sokkal több információt és megszámlálhatatlan csatornán képes hozzájuk eljuttatni, pillanatok alatt, akár „valós időben". Az internet tehát mind hatása, mind szolgáltatásainak újszerűsége miatt megkerülhetetlen felület az alkotmányjog számára. Az internet vagy gyakran az „online" világ megítélésének a főbb kérdései témánk szempontjából a következők.[13]

Elhatárolási kérdéseket vet fel a médiatartalom-szolgáltatások és az egyéb internetes kommunikáció jelensége, továbbá tisztázandóak szabályozásuk eltérései. Megállapítható, hogy az interneten is támogatandó a véleménynyilvánítás szabadságának érvényesülése. Frank La Rue, az ENSZ különmegbízottja megállapítja, hogy a Polgári és Politikai Jogok Nemzetközi Egyezségokmányának 19. cikkét már azzal az előrelátással szövegezték, hogy a technikai fejlődés révén később kialakuló minden lehetséges felületen biztosított legyen a véleményszabadság.[14]

Jelen dolgozat témáját tekintve az internetet mint olyan felületet fogjuk fel, amely a politikai diskurzusok számára teret kínál. A téma kidolgozása miatt szükséges megjegyezni, hogy az interneten olyan szolgáltatások és tartalmak is megjelennek, amelyek a médiaszabályozás hatálya alá tartoznak, de most az egyéb tartalmakra és

[12] Koltay: i. m. (2012) 487, 506. o.

[13] Az internet jogi szabályozásának további kapcsolódó problémáit áttekinti: Bartóki-Gönczy Balázs – Pogácsás Anett: A médiatartalom-szolgáltatásnak nem minősülő internetes tartalmak szabályozása. In Koltay András – Nyakas Levente (szerk.): *Magyar és európai médiajog.* Budapest, Complex, 2012, 581–605. o.; valamint Bernd Holznagel: Internet freedom, the public sphere and constitutional guarantees. In Monroe E. Price – Stefaan G. Verhulst – Libby Morgan: *Routledge Handbook of Media Law.* London/New York, Routledge, 2013, 141–156.

[14] *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Frank La Rue. United Nations General Assembly, 2011. (A/HRC/17/27) 7. (https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf). Az európai jogvédelem szempontjából hasonlóképp lásd *Freedom of Expression and Democracy in the Digital Age Opportunities, rights, responsibilities. Political Declaration and Resolutions.* Belgrade, CoE, 2013. (https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680484e65).

kommunikációs elemekre kell fókuszálnunk, így különös jelentőséggel bír a közösségi médiának vagy web 2.0-nek („webkettőnek") nevezett jelenség.

Azokat a tartalmakat és formákat is a politikai diskurzus részeinek tekintem, amelyek talán nem a médiaszabályozás fogalma alá eső tömegkommunikáció elemei, de szociológiai értelemben nagyon hasonló funkciót töltenek be. Meglehet, a felhasználók jelentős köre nem kíván részt venni a politikai diskurzusokban, inkább csak szórakozásra, magánéleti kapcsolatok ápolására használja az internet nyújtotta lehetőséget. Azonban a két szféra, a felhasználók interaktív közreműködésén, tartalomszolgáltatásán alapuló közösségi és a hagyományos, profi tömegkommunikációs média elhatárolása nehéz. „[...] a kettő egyre inkább összemosódik – egy-egy politikai vita kapcsán a közösségi oldalakat szinte elárasztják a szórakoztató videók, bejegyzések, kommentek, stb., amelyek elősegítik a véleménypluralizmust, és kétség kívül komoly véleményformáló hatással is bírnak."[15] Az ENSZ szakmai jelentése úgy fogalmaz, hogy az újságírók védelmére szolgáló intézkedéseket ki kell terjeszteni a nem professzionális, ún. „civil újságírókra" is, hiszen ők, a hétköznapi emberek is jelentős és fontos információt oszthatnak meg egy adott helyzetben.[16]

Szabályozási kérdéseket vet fel az interneten elérhető anonimitás. A hozzászólók bátrabban nyilvánítanak véleményt, amennyiben személyüket nem kell felfedniük, ez még a demokratikus viták minőségét is támogatni látszik – hiszen érvek ütköznek, a véleményt formáló személy szociális és egyéb hátterére tekintet nélkül. Azonban az anonimitás a jogsértőnek vagy egyébként károsnak minősülő megnyilvánulásokra is bátorítást adhat, márpedig a véleményszabadság korlátait az interneten is számon lehet kérni.[17]

A kérdés az, hogy az anonimitás és a jogérvényesítés egyéb nehézségei (pl. a joghatóság problémája a globális szolgáltatások kusza valóságában) révén jelentkezik-e az internetes kommunikáció nagyobb szabadsága, vagy sajátos jogi rezsimről beszélhetünk-e. A „hagyományos" kommunikációjogi szabályozás kiterjedt alkalmazásának próbakövei az interneten közzétett tartalmakért való felelősség sajátos esetei. Ezek egyik központi kérdése, hogy az internetes szolgáltatók különféle körei felelősséggel tartoznak-e olyan tartalmakért, amelyeket nem ők hoztak létre, de azok a tartalmak olyan felületen jelentek meg, amelyeket ők alkottak vagy működtetnek (lásd közvetítő szolgáltatók felelőssége, web 2.0 felületeket működtetők felelőssége, kommentekért és blogokért való felelősség kérdései).[18]

Sokan a szabad internet paradigmája alapján a közvetítő szolgáltatók, illetve a közösségi diskurzus felületeit biztosítók (legyen az akár a kommentelést lehetővé

[15] Bartóki-Gönczy–Pogácsás: i. m. (2012), 587. o.

[16] Lásd a Protection of „citizen journalists" címszó alatt, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. UN General Assembly, 2010.

[17] Bartóki-Gönczy–Pogácsás: i. m. (2012) 588. o.

[18] Részletesebben Bartóki-Gönczy–Pogácsás: i. m. (2012), 595–601. o.

tevő internetes újság) korlátozott felelőssége mellett kardoskodnak. Amennyiben a jogsértő tartalomra megfelelő eljárásban felhívják ezek figyelmét, és ez alapján intézkednek az eltávolításról vagy a jogsérelem megszüntetéséről, akkor mentesülésük elfogadható („*notice-and-take-down*" rendszer).[19] Akár a tartalomfeltöltés üzemszerű szűrése, akár a felhasználók anonimitásának tagadása megoldást kínálhatna, igaz, ez némileg szemléletváltással – és extra költségekkel – járna az internet világára nézve, s gyakorlati megvalósíthatóságával kapcsolatban komoly kétségek merülhetnek fel. Hacsak nem a kommentelési-hozzászólási lehetőségek teljes felszámolását választják. Ez azonban az öncenzúra el nem fogadható változatának tekinthető, és a demokratikus diskurzusok modern felületeinek drasztikus sérelmével járna. Ez az „öncenzúra" (valójában magáncenzúra) azért veszélyes, mert a tartalomszűrést magáncégek végeznék, jogilag nem követhető és nem átlátható módon. Már korábban megfogalmazódott, hogy a közvetítő szolgáltatást és felületeket nyújtó magánvállalatoknak alapvetően csak bírósági határozatok alapján kellene beavatkozniuk a kommunikációs folyamatokba, és az ilyen intézkedéseik is legyenek teljesen transzparensek, a visszaélések megelőzése érdekében.[20]

A politikai diskurzusokban és a közvélemény formálódásában kiemelkedő szerepet játszanak a közösségi média felületei. Ezeket nem lehet minden esetben szigorúan elválasztani a magánkommunikáció-tömegkommunikáció elvén, mint ahogyan azt a nem eléggé alapos indokolásában a 19/2014. (V. 30.) AB határozat megtette. Az Alkotmánybíróság ebben a döntésében az internetes kommentekért való felelősséget kiterjesztette a topikokat működtetőkre is, tekintet nélkül arra, hogy a kifogásolható, jogsértő hozzászólásokat később szűrték és eltávolították – miközben az internetes kommunikáció körében ismételten elzárkózott a közösségi oldalak és blogok vizsgálatától. A többségi indokolás szerint ugyanis az Alaptörvény IX. cikke a nyilvános szólást védi, a közösségi oldalak hozzászólásai, posztjai pedig regisztrációval érhetőek el, és szűrhető személyi kör számára szólnak.[21] (Az AB nem látta továbbá fennállni a médiatartalom fogalmi elemeit – gazdasági szolgáltatási jelleg, tájékoztatási-oktatási-szórakoztatási cél, nyilvánossághoz való eljuttatás célja, szerkesztői felelősség – sem.) Valójában ez a webkettő időszakának, a virtuális közösségi lét sajátosságainak tényleges megfontolása nélkül fogalmazódott meg. A közösségi oldalakon a magánszféra technikailag konstruálható ugyan, de a praktikus tapasztalat az, hogy ezeket a fórumokat mozgalmak, pártok, politikusok, sajtó- és médiaszervezetek, általában közéleti szereplők intenzíven használják. Az

[19] A szolgáltató különös gondosságáról szól viszont a strasbourgi bíróság döntése a *Delfi AS v. Estonia, 2015* (Application no. 64569/09) ügyben.

[20] Lásd már a Frank La Rue jelentésben is (A/HRC/17/27) 11–14. o.

[21] 19/2014. (V. 30.) AB határozat [61]. Az AB nem látta továbbá fennállni a médiatartalom fentebb leírt fogalmi elemeit (gazdasági szolgáltatási jelleg, tájékoztatási-oktatási-szórakoztatási cél, nyilvánossághoz való eljuttatás célja, szerkesztői felelősség) sem.

AB határozat ezt a tényt, mint kivételt, megemlíti, de semmilyen további következtetést nem fűz hozzá.[22]

A hozzászólások szolgáltatók általi előzetes moderálása lehet kimentő körülmény, ám ezzel az AB határozata a kommentelésben megnyilvánuló diskurzus mint műfaj szolgáltatók általi általános korlátozását vetíti előre. A kommentekért való szolgáltatói felelősség megállapítása miatt ily módon ez a restriktív döntés az „internet szabadságának" romantikus felfogását áttolja a „Facebook romantikus szabadságának" felfogására. Mindazonáltal a rendes bírósági gyakorlat, például a személyiségi jogi perekben, rágalmazási-becsületsértési tényállások esetén, a közösségi hálón a nagy nyilvánosság megvalósulását meg tudja állapítani, illetve cizelálltan megközelíteni.[23]

Az internet nemcsak a politikai diskurzusok számára kínál felületet, hanem forrásul, információs svédasztalként is szolgálhat. A közérdekű adatok közzététele az interneten hatalmas lehetőségeket kínál az információszabadság fejlődése számára.[24] Ez abban áll, hogy egyre nehezebb lesz technikai nehézségekre hivatkozni, ha egy állami szerv működésére, kezelésében levő adatokra vonatkozó közzétételi kötelezettség ellenében próbálunk érvelni. Ebből a szempontból a honlapok működtetésének és naprakészen tartásának rendkívül alacsonyak a határköltségei, míg a közügyek iránt érdeklődő polgárok és újságírók számára az adatokhoz való hozzáférés válik – anonimitásával, ingyenességével stb. – egyszerűvé.

3. A POLITIKAI DISKURZUSOK TORZULÁSA AZ ONLINE TÉRBEN – ÉS A LEHETSÉGES VÁLASZOK

3.1. A torzító tényezőkről

A politikai diskurzusok kommunikációs mezejében torzítóként megjelenő tényezők és magatartások számbavétele a demokratikus eljárások védelméhez szükséges alkotmányos garanciák, technikai eszközök-megoldások azonosításához is hozzájárul. Ezen tényezők között tekinthetjük át az állami/közhatalmi beavatkozásokat, a gyakran globális hálózattal és befolyással bíró online közvetítők/kapuőrök szerepét, a hazai vagy külföldi rossz szándékú szereplők tevékenységét, de egyes társadalmi kulturális-szociálpszichológiai mintázatokat is.

[22] Hasonló kritikai szellemben lásd Stumpf Istvánnak a határozathoz fűzött különvéleményét.

[23] Lásd a Budapest Környéki Törvényszék P.20417/2020/18. számú határozata sérelemdíj tárgyában (2021. október 27.).

[24] Az EU Tanácsa által 2014 májusában elfogadott *„EU Human Rights Guidelines on Freedom of Expression Online and Offline"* is megemlíti az információkhoz való hozzájutás internetes lehetőségeit; ennek ellenére kritikáját lásd: EU Expression Guidelines Fail to Recognise the Right to Information. *Article19, 2014.* (https://www.article19.org/resources/eu-expression-guidelines-fail-recognise-right-information/).

A kormányok az internet globális lehetőségeiben egyszerre találhatnak fejlesztési perspektívát (jó állam szolgáltatásai, tájékoztatás,[25] stb.) és kockázatokat. Még a demokratikus rendszerek is többször nyilvánvaló ellenségnek tekintik az internetes szabadság köreit, amely felerősíti a nemzetbiztonságra leselkedő veszélyeket. Ezért világszerte elterjedt az internetes tartalmak szűrése, sőt az internethez való hozzáférés korlátozása.[26] Ezek körében emlékezzünk a véleményszabadság elfogadott korlátaira, amelyek alapján a tartalmi szűrési szempontok demokratikusan igazolhatóak lehetnek (pl. a gyermekpornográfia).[27]

Az említett emberi jogi előnyök, a demokrácia és a szabadságjogok erősítésének lehetősége miatt felmerült, hogy az internethez való jogot emberi jogként kellene elismerni és védeni.[28] Mivel technikailag nemcsak a tartalomszűrés vagy az internetforgalom ideiglenes korlátozása képzelhető el, hanem az is, hogy egy ország teljes egészében lekapcsolja az internetet („internet kill switch"), a kérdés az emberi jogok legújabb generációjának valós problémájává válik. A világhálóhoz való hozzáférés szabadsága igazolható a véleménynyilvánításhoz, a tájékozódáshoz, az önmegvalósításhoz való jog alapján is, de a nyugati demokráciák társadalmainak kiterjedt gazdasági-közéleti internetfüggése révén is. Néhány országban[29] már regisztrálhatunk jogi szabályozási előrelépéseket, ezek mind erősítik a világháló azon demokratikus ismérveit és előnyeit, amely szerint szinte költségek nélkül, bárki bekapcsolódhat a politikai diskurzusokba, ott véleményt formálhat, információt oszthat meg és szerezhet.[30]

Koltay szerint tényként kezelhetjük, hogy az internetes közvetítő szolgáltatók „nem passzívan viszonyulnak a mások által készített tartalmakhoz, hanem annak egyfajta »szerkesztői« részben saját akaratukból (például a Facebook moderálási elvei és a tartalmakat a felhasználó elé juttató algoritmusok beállítása), részben a jog

[25] Az internet és az infokommunikációs technológiák a demokratikus eljárások új modelljének felvázolásához is forrásul szolgálhatnak. Az információtechnológiát a kormányok az állampolgárok részvétele és döntéshozatalba való bevonása céljából fejleszthetik, a másik oldalról a közvetlenül döntést hozó polgárok közötti koordinációt is megvalósíthatja. Lásd Mateus de Oliveira Fornasier: The Realization of E-Democracy in the 21st Century. *Revista da Faculdade de Direito da Universidade Federal de Minas Gerais*, 2021/jan–jun. 259–284. o.; Tero–SæbØ Øystein Päivärinta: Models of E-Democracy. In *Communications of the Association for Information Systems,* 2006/1. szám.

[26] Lásd több ország gyakorlatát, a Reporters Without Bordersnek „az internet ellenségeiről" szóló összeállításában. (https://rsf.org/sites/default/files/2014-rsf-rapport-enemies-of-the-internet.pdf).

[27] A Frank La Rue jelentés ezt tekinti a tartalomszűrés egyetlen elfogadható indokának, lásd 9–10. o.

[28] Álvarez Robles Tamara: Las garantías de los derechos fundamentales en y desde la red: El contexto español: consideração especial do contexto espanhol. *Revista Chilena De Derecho Y Tecnología*, 2022/1. szám, 5–40. o.

[29] Még az Európai Unió gazdasági érdekekből kiinduló 2002/22/EK irányelve (Egyetemes szolgáltatási irányelv) is tartalmaz erre utaló elemeket.

[30] Nicola Lucchi: Freedom of expression and the right of access to the Internet. A new fundamental right? In Monroe E. Price – Stefaan G. Verhulst – Libby Morgan: *Routledge Handbook of Media Law*, London/New York, Routledge, 2013, 157–173. o.

által kötelezetten (jogsértő tartalmak törlésére kötelezés)". A megközelítésünk – a közönség, a politikai közösség tagjainak kommunikációs folyamatai – szempontjából pedig jelenlegi dogmatikai alapjainkon érvényes probléma a tartalom-előállítók hozzáférése a közvetítő szolgáltatásokhoz, a közönséghez való eljutás lehetősége az online platformokon. „Ennek jogi megalapozása a korábbi doktrínák alapján nehézkes, hiszen a közvetítők jellemzően magántulajdonban álló vállalkozások, így a jog csak kivételes esetben tudja őket kötelezni a médiaszabályozásból ismert hozzáférési jogok (például sajtó-helyreigazítás) biztosítására vagy más közérdekű kötelezettségek (például közügyekkel kapcsolatos tájékoztatás) teljesítésére – egyelőre csak az internetszolgáltatók hálózatsemlegessége ügyében lehet hasonlóra (az egyenlő hozzáférés biztosítására) jogi alapot találni."[31]

Az online szolgáltatók „kapuőri" szerepe és az abból adódó hatalmi pozícióik megannyi terepen azonosíthatók. Klasszikus jogi fogalmaink – szól Kadri figyelmeztetése – egyszerre hívják fel a kapuőrök korlátozó szerepére és a pozícióikat védő jogokra a figyelmet.[32] A kapuőrök megannyi adatot gyűjtenek – és ezen adatok felett úgy rendelkeznek, hogy azok tárolásával, megosztásának felügyeletével-manipulálásával az adatbázisok értékét önmaguk formálják. Az online platformok a szolgáltatási környezetük meghatározása során szuverén módon döntenek egyes kiegészítő szolgáltatásokról, azok átjárhatóságáról-kompatibilitásáról, így érdemben befolyásolni tudják a digitális innovációs ökoszisztémát. Az online keresőmotorok továbbá érdemben képesek meghatározni az információhoz való hozzájutásunkat, rangsorolva vagy éppen szűrve a találati eredményeket. Ennek bázisán pedig a felhasználók buborékba zárása (csak bizonyos, célzott adattartalmakhoz való hozzáengedése) is megvalósul.[33] A közösségi média természeténél fogva személyes adatok megosztására buzdít minden felhasználót, azzal a *korántsem* teljes megnyugvást nyújtó ígérettel, hogy adatainkat nyomon követhetjük, a hozzáférők körét korlátozhatjuk, stb.

Az online kommunikációs közeg felhasználói között jó és rossz szándékúakat egyaránt találunk. A rossz szándékúak az internet szabadságát jelentő jogi és technológiai lehetőségeket, a felhasználók attitűdjeit és szociálpszichikai motívumait egyaránt használják, kihasználják. Témánk szempontjából az egyéni jogsérelmeken

[31] Koltay András: Az internetes kapuőrök és az Emberi Jogok Európai Egyezményének 10. cikke – a sajtószabadság új alanyai. *Állam- és Jogtudomány*, 2017/4. szám, 139–140. o.

[32] Thomas E. Kadri: Digital Gatekeepers. *Texas Law Review*, 2021/5. szám, 951–1004. o. Kadri szerint „rókákra bíztuk a tyúkól őrzését". A magyar szakirodalomban összefoglalóan: Bartóki-Gönczy Balázs: *Az online közvetítő szolgáltatók mint az információhoz való hozzáférés új kapuőrei.* Budapest, Pázmány Press, 2018.

[33] Felvethető ezen mondat passzív megfogalmazása: a felhasználók buborékba kerülnek, stb., amennyiben a következményeket adott magatartások következményének tekintjük. Lehet az algoritmusok eredménye, de felfogható úgy is, hogy a felhasználó tevékenységének olyan eredményéről beszélhetünk, amely az algoritmusok működési mechanizmusainak ismeretében előre kiszámítható.

(zaklatás, adathalászat stb.) túli, a közösségi informálódás és demokratikus eljárások problémáit kell érintenünk. Ebben a kérdéskörben a legkézenfekvőbb esettanulmányokat a választási kampányokba való „beavatkozások" szolgáltatják.[34]

A nemzetközi közéletben és a szakirodalomban a legnagyobb hullámokat az orosz trolloknak a 2016-os amerikai elnökválasztási kampányban való megjelenése (beavatkozása) generálta. A szóban forgó választási kampányban az álhírek társadalompszichológiáját és a külföldi beavatkozást („election meddling" vagy „interference") egyaránt szemügyre vehetjük. Ez utóbbiakat tényszerűen dokumentálni éppoly nehéz, mint tételesen kimutatni a hatásukat a szavazatok alakulására.[35] A helyzet sajátossága, hogy a kibertérben tevékenykedő trollok/hackerek Oroszország kormányzati berendezkedése nyomán a tevékenységek mögött állami támogatás áll(hat), továbbá a volumenek nagy létszámú hacker által kifejtett üzemszerű[36] akcióra utalnak. Az amerikai National Intelligence Council 2021-es jelentése a 2020-as választásokról (visszautalva a 2016-os hasonlóságra)[37] mindazonáltal fontos megállapítást tesz: Oroszország azonban nem próbálta „megváltoztatni a szavazási folyamat bármely technikai aspektusát, beleértve a szavazók regisztrációját, a szavazatok leadását, a szavazatszámlálást vagy az eredmények közlését". Ehelyett az „online befolyásolás szereplői arra törekedtek, hogy befolyásolják az amerikai közvéleménynek a jelöltekkel kapcsolatos megítélését, valamint előmozdítsák Moszkva régóta fennálló céljait, vagyis az amerikai választási folyamatokba vetett bizalom aláásását és az amerikai nép társadalmi-politikai megosztottságának növelését".[38] Az Egyesült Államok általános, és globális érdeklődésre számot tartó választási kampányai újabban hozzásegítették a közvéleményt, hogy ráeszméljen az internet adta befolyásoló, rosszindulatú tevékenységekre. Mert noha ahogy azt Kovács és Krasznay megfogalmazzák, ugyan „a trollkodás egyidős az internettel, azonban tudatos politikai felhasználása csak néhány évre

[34] Kovács László – Krasznay Csaba: „Mert övék a hatalom": Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során. *Nemzet és Biztonság*, 2017/3. szám, 3–15. o., Daniel Mack: An Era of Foreign Political Interference: Impulsive, Overcompensation of Australia, and a Comparison of Legislative Schemes with the United States. *Emory International Law Review*, 2020/1. szám, 367–398. o.

[35] Kronologikus gyűjtést nyújt az egyes kibertéri tevékenységekről: Kovács–Krasznay: i. m. (2017), 3–6. o.

[36] Bányász Péter – Dobos László – Palla Gergely – Pollner Péter: Lélektani műveletek a közösségi médiában. In Auer Ádám – Joó Tamás (szerk.): *Hálózatok a közszolgálatban.* Budapest, Dialóg Campus, 2019, 119. o.

[37] National Intelligence Council: *Foreign Threats to the 2020 US Federal Elections*. 2021, ICA 2020-00078D. (https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf).

[38] Idézi Michael N. Schmitt: Foreign Cyber Interference in Elections. *International Law Studies Series. US Naval War College,* 2021, 740. o.

tekint vissza"[39], valójában ennek a hatásnak a felerősödése a közösségi média felhasználói körének attitűdjeihez köthető.

A választási-politikai meggyőző tevékenység (hívjuk akár politikai kommunikációnak, akár befolyásolásnak) paradigmaváltása szembeötlő, és a politikai aktorok által tudatosan használttá vált eszközökön, a politikai közösség tagjainak politikai kultúráján alapszik. Az emberi tulajdonságok (magamutogatás, elismerésre és figyelemre vágyódás stb.) mellett a társadalmi nyilvánosság újabb, immár hitelességi szerkezetváltozására is fel kell hívni a figyelmet, hiszen „az online médiatartalmak felgyorsították a hírek áramlását, ami hatással volt a hírek előállítására és a hírciklusra, ami elvezetett az újságírói szakma változásához. Az úgynevezett copy-paste (másol-beilleszt) újságírás a megbízhatónak gondolt hírek kritika nélküli átvételét jelenti, ami kielégíti a folyamatos híráramoltatás elvárását. Hátulütője ennek, hogy az újságírók kapuőri szerepe elveszik és könnyebbé válik a hírek befolyásolása a külső szereplők által, aminek hatására a hírszolgáltatók hitelessége is csökken. Manapság sokkal egyszerűbb megkérdőjelezni egyes hírszolgáltatók pontosságát, mint korábban."[40] Ebben a társadalmi közegben a demokratikus eljárásokba vetett bizalmat általában is könnyű megingatni.

A szerkesztői felelősség hiánya a tömegkommunikációs mezőben egy kapuőrszereplőt iktat ki – ennek pedig következménye a közvélemény roncsolódása. Egyes jelenségek messze valós jelentőségüktől eltérő súllyal tűnnek fel a diskurzus- vagy nyilvánosság-mezőben, ez pedig félrevezető lehet a közügyek valós elemeinek és alakulásuk megítélésében.[41] A jogi megítélés nehézsége, hogy ebben az esetben ritkán találunk jogaiban sértett személyeket, akik alapjogi igényeik érvényesítése miatt fellépnek, sokkal inkább „közérdekvédelmi" megítélésre volna szükség. Olyan kérdésekben viszont, hogy mely bűncselekmények szaporodtak el, van-e „közbiztonság", fenyeget-e a globális felmelegedés, hanyatlik-e a „Nyugat", stb. valójában egy szerteágazó, többszereplős diskurzus adhatna valamilyen valóshoz közelítő képet. Az egyes hozzászólásoknak minősíthető felhasználói tartalmak önmagukban sem,

[39] Kovács–Krasznay: i. m. (2017), 14. o. Vagy, mint a didaktikusan magyarázó német szövetségi tájékoztató oldal összegzi, a téves tájékoztatás (misinformation) régebben tapasztalt jelenségeihez képest a félretájékoztatás (disinformation) lényege, hogy „a félrevezető és téves információk azonban akkor válnak veszélyessé, ha céljuk az emberek szándékos megtévesztése vagy befolyásolása, és célzottan terjesztik őket. A mögötte álló szándék tehát a lényeges különbség a dezinformáció és az álhírek között." A dezinformáció esetében a tartalom manipulált (deepfake, hamisított fotók, hamis honlapok), kontextusból kiragadott (rövidített idézetek, téves statisztikák) vagy éppen tisztán fiktív (https://www.bundesregierung.de/breg-de/themen/umgang-mit-desinformation/disinformation-definition-1911048).

[40] Merkovity Norbert: *A figyelemalapú politika a közösségi média korában. A politikai kommunikáció lehetséges értelmezése napjainkban.* Budapest, Médiatudományi Intézet, 2018, 86. o.

[41] Mezei Kitti – Szentgáli-Tóth Boldizsár: Az online platformok használatában rejlő veszélyek: a dezinformáció és a kibertámadások jogi kockázatai. In Török Bernát – Ződi Zsolt (szerk.): *Az internetes platformok kora.* Budapest, Ludovika Egyetemi Kiadó, 2022, 329–330. o.

és megosztásukkal mérhető hatásukban sem ítélhetők meg egykönnyen. Ezek a dezinformációs tartalmak ráadásul nemcsak nem szerkesztettek, de sokszor nem is valós személyek, hanem botnetek által létrehozottak, terjesztettek.[42]

3.2. Egyes szabályozási válaszok

A fentebb említettek alapján, az online térben (mint napjaink jellemző felületén) folyó diskurzusokat a demokratikus és alkotmányos standardoktól több tényező téríti el; pusztán az egyes jelenségekre vagy szereplőkre partikulárisan hatni kívánó fellépés nem lesz hatékony. Mint ahogyan annak felismerése is fontos, hogy az állami szuverén szabályozó hatalma úgy a globális szereplők irányában, mint a határon túlról érkező befolyásoló tevékenységek tekintetében – bizony érdemben korlátozott.

Napjaink legfontosabbnak tartott szabályozási eredménye az Európai Unió Tanácsa és Parlamentje által 2022-ben elfogadott Digital Services Act.[43] Ez nemcsak az érintett tagállamok és lakosság száma alapján lehet hatásos, de megközelítése kellően cizelláltnak mondható. Alaptétele, hogy „a biztonságos, kiszámítható és megbízható online környezet biztosítására vonatkozó célkitűzés elérése érdekében e rendelet alkalmazásában a jogellenes tartalom fogalmának nagyjából az offline környezetre vonatkozóan létező szabályokat kell tükröznie" (Preamb. [12]). A digitális szolgáltatások szerteágazó területei közül a témánk kapcsolódási pontját a preambulum (82) bekezdése fogalmazza meg, amely egyértelmű kockázatként azonosítja azokat a negatív hatásokat, amelyek „a demokratikus folyamatokra, a polgári közbeszédre és a választási folyamatokra" irányulnak.[44] Az egyes diskurzustorzító jelenségek közül megemlíthetjük a buborékképző, algoritmusok által generált információhoz jutást, ennek kapcsán a rendelet korlátozni törekszik a profilalkotáson alapuló szolgáltatásnyújtást, például kiskorúak vagy a GDPR szerinti különleges adatok esetében.

[42] Botnetek bemutatásához lásd Bederna Zsolt – Váczi Dániel – Pollner Péter – Szádeczky Tamás: Támadás hálózatba szervezve. In Auer Ádám – Joó Tamás (szerk.): *Hálózatok a közszolgálatban.* Budapest, Dialog Campus, 2019, 223–247. o. Bár empirikus kutatások azt is igazolni vélik, hogy a természetes személyek hatékonyabban terjesztenek álhíreket, mint a botnetek, lásd Bányász et al. (2019) 119. o.

[43] 2022/2065 rendelet (2022. október 19.) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (digitális szolgáltatásokról szóló rendelet, a továbbiakban: DSA). (https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32022R2065&from=EN).

[44] További kockázati kategóriák a rendelet értelmében: jogellenes tartalmak – például gyermekek szexuális bántalmazását ábrázoló anyagok vagy jogellenes gyűlöletbeszéd – terjesztése, a jogellenes tevékenységek folytatása, az EU Alapjogi Chartája által védelmet élvező alapvető jogok érintettsége (különösen, hogy a kiskorúak mennyire lehetnek kitéve olyan tartalmaknak, amelyek károsak egészségükre, valamint fizikai, szellemi és erkölcsi fejlődésükre), tartalmak, amelyek a személyek, különösen kiskorúakkal szemben nemi alapú erőszakot eredményeznek, vagy például a közegészséggel kapcsolatos összehangolt dezinformációs kampányok hatásai (DSA 34. cikk).

A DSA határozott kíván lenni abban a tekintetben, hogy az Unió területén működő szolgáltatóknak, óriásplatformokat s „nagyon népszerű" online keresőprogramot üzemeltető szolgáltatóknak közre kell működniük a kockázatok azonosításában és kezelésében egyaránt. Ennek érdekében uniós és tagállami jelzési mechanizmusok létesülnek, továbbá a szolgáltatók független ellenőrzésen esnek át (36–37. cikk). Az Unió alapállása, hogy a szolgáltatók társszabályozásának helyet ad, ösztönözve őket önkéntes magatartási kódexek (45. cikk) és válságkezelési protokollok (48. cikk) kidolgozására – különösen közbiztonságot vagy közegészségügyet érintő rendkívüli válsághelyzetekben, így járványok vagy háború idején. A tagállamok meghatározhatják a hatáskörükbe tartozó esetekben „a hatékony, arányos és visszatartó erejű" szankciók körét és végrehajtását (52. cikk).

A tagállami fellépésekhez nem kellett különösebb impulzust adni, arra már találhattunk példákat eddig is. 2019-ben a dezinformációval szembeni közös cselekvési terv végrehajtásáról szóló jelentés nem túl optimista helyzetértékelése további uniós és tagállami intézkedéseket sürgetett.[45] Németország 2017-ben fogadta el azt a törvényt (NetzDG), amely jogérvényesítés előmozdítását célozta a közösségi hálózatokon, s amely jelentős mértékű bírsággal fenyegette azt a szolgáltatót, amely nem tesz eleget a jelentési kötelezettségének, és a jogszerűtlen (pl. gyűlöletkeltő) tartalmak eltávolítását elmulasztja.[46] 2020-ban Franciaországban 24 órás eltávolítási kötelezettséget írtak elő a bejelentett és jogsértő tartalmak tekintetében (az ún. Avia-törvény a német szabályozást követte); jóllehet a francia Alkotmánytanács jó néhány rendelkezését megsemmisítette, mivel a szólásszabadság alkotmányellenes korlátozásának tekintette.[47]

Végezetül meg kell jegyeznünk, hogy a politikai diskurzusok minőségével, a dezinformáció megelőzésével kapcsolatos akcióknak nyilvánvaló ki kell terjednie a nevelésre is. Különösen az iskolai, de más szocializációs közegek (beleértve a civil szervezeteket) felelőssége és támogatása is szükséges.[48]

[45] Az EU Bizottsága és a külügyi és biztonságpolitikai főképviselő közös jelentése, JOIN(2019)12, elérhető: https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=comnat:JOIN_2019_0012_FIN.

[46] Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act), 2017. Elérhető: https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf;jsessionid=829D39DBDAC5DE294A686E374126D04E.1_cid289?__blob=publicationFile&v=2.

[47] Decision no. 2020-801 DC of 18 June 2020, Constitutional Council, https://www.conseil-constitutionnel.fr/decision/2020/2020801DC.htm. Ld. még: Freedom House: *Freedom on the Net 2021, France* – https://freedomhouse.org/country/france/freedom-net/2021.

[48] Az Európai Unió akciója tekintetében lásd: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6048 illetve a hazai akciókról az NMHH kampányát: https://nmhh.hu/cikk/214271/Ne_hagyd_hogy_a_hireket_olvasva_becsapjanak_az_erzelmeid.

4. KONKLÚZIÓ

A politikai diskurzusok online térben való vizsgálata során meg kellett állapítanunk, hogy a klasszikus értelemben vett kommunikációs jogok az interneten is alkalmazásra kerülhetnek. Az alapjogi védelem sajátos interferenciában van az internetes szolgáltatók jogosultságaival vagy másképp speciális helyzetükkel. Egyszerre kínálnak „nagyobb teret" diskurzusoknak és szolgáltatásaik az egyén politikai kommunikációs közegben való elbizonytalanodását, elmagányosodását. Ezért központi célpontjai úgy a jogalkotási kezdeményezéseknek (felelősségtelepítés, társszabályozás), mint a bírói jogalkalmazás jogértelmezési feladatainak. Ugyanakkor az állam intézményvédelmi szerepére is felhívtuk a figyelmet: témánk szempontjából nemritkán nehezen azonosítható személyes jogsérelem, amikor közérdekvédelmi feladattá válik a félrevezető tartalmak és demokratikus közvéleményt különféle módon torzító tevékenységek elleni fellépés. Az Unió legújabb DSA szabályozását valóban markáns eredménynek tarthatjuk (különösen a tagállamok és egyéb érdekeltek, stakeholderek közötti egyetértés tekintetében), azonban hatékonyságát, alkalmazhatóságát majd választási eljárások és egyéb kampány- vagy válságesemények során kell tesztelni. Jelentős esélye van annak is, hogy a technológiai fejlődés újabb eredményeit lesznek képesek a rosszindulatú aktorok a saját céljaikra fordítani, így pedig a komplex, de rugalmasan alkalmazható jogi megoldások kínálhatnak csak versenyképes megoldásokat az ilyen befolyásolásokkal szemben.

Mivel a bemutatott diskurzusszabályozásokkal kapcsolatban alapelvi szinten szubsztantív érvek állnak az egyéni alapjogvédelem és a közérdekvédelem oldalán is, nagy valószínűséggel paradigmatikus szemléletváltásra volna szükség az internet szabadságának romantikájával szemben.[49] A szemléletváltás elvi modelljét a militáns demokrácia adhatja. A militáns vagy önvédelemre képes demokrácia jelszavát a rendszerellenes politikai pártokkal szemben fogalmazta meg a német szövetségi alkotmánybíróság, majd más testületek, míg az alkotmánytani szakirodalom is érvényes (kvázi normatív) modellként kezeli. A szabad pártalapítás és a pártok egyenlőségének meghaladásával volt lehetséges fellépni a politikai szabadságjogokat a demokratikus alkotmányos rendszer lebontására használni törekvő szervezetekkel szemben.[50] Az új szemlélethez köthető megoldási javaslatokból nincs hiány. Az anonimitás megszüntetése, a sajátos (különösen közéleti hírekről szóló) tartalmak megosztásának tiltása, stb. a szolgáltatók és az állam kapcsolatának újratervezését jelenti. Viszont hogy a demokratikus politikai diskurzusok sokszínűségét, az abban való részvétel egyenlőségét, az alternatív információforrások kiegyensúlyozottságát tekintve a bizalom és igény létezik-e egy politikai közösségben, az már más lapra tartozik.

[49] Sikerük esetén nevezhetjük a „hőskor" végének is a különböző irányú törekvéseket, lásd Bede Márton: *Az internet hőskorának vége* (https://444.hu/tldr/2017/07/18/az-internet-hoskoranak-vege).

[50] Bővebben lásd Smuk Péter: *Magyar és európai pártjog.* Budapest, Gondolat Kiadó, 2018, 107–115. o.

GOSZTONYI GERGELY

Az államok által végzett internetkorlátozás különböző eszközei mint nemzetbiztonsági és szólásszabadsági kockázatok*

IYNAYNPA[1]

2022-ben a Freedom House internetről szóló éves jelentésében így fogalmazott: „A vizsgált országok több mint kétharmadában a hatóságok jogi és szabályozási hatáskörükkel korlátozzák a külföldi információforrásokhoz való hozzáférést, így a lakosok egy olyan hazai információs térben maradnak, amelyet gyakorlatilag az állam alakít."[2] A helyi szabályozások egyre inkább megfigyelhető zavarai összefüggenek az internetszuverenitás kérdésével, és együtt befolyásolják a szólásszabadságért folyó küzdelmet. Az egyre inkább terjedő cenzúra fogalmának szűk és tág értelmezési keretei pedig az alul- és túlhasználat veszélyeire figyelmeztethetnek. Mindezek mellett – ahogy Romain Badouard fogalmaz *A web új törvényei* című 2020-as könyvében – a jogi fogalmak sokszor „elég homályosak ahhoz, hogy nagyon különböző típusú beszédet foglaljanak magukban, potenciálisan megnyitva az utat az online tartalomszabályozás politikai instrumentalizálása előtt".[3] Az állami szabályozás így válik elkerülhetetlenné,[4] és ennek az internet nemzetközi jellegéből adódóan – félő – sok esetben lesznek járulékos veszteségei is.

* A Bolyai János Kutatási Ösztöndíj és a Kulturális és Innovációs Minisztérium ÚNKP-23-5 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

[1] Internetes közmondás (If you're not angry, you're not paying attention) rövidítése: Ha nem vagy dühös, akkor nem figyelsz.

[2] Freedom House: *Freedom on the Net. Countering an Authoritarian Overhaul of the Internet*, 2022. október 18., https://freedomhouse.org/sites/default/files/2022-10/FOTN2022Digital.pdf, 11. o.

[3] Romain Badouard: *Les nouvelles lois du web. Modération et censure*, Paris, Le Seuil, 2020, 13. o.

[4] Vö.: „Most azonban teljesen lehetséges, hogy a végső cyberlord maga a kormányzat." Alfred C. Yen: Revisiting the Western Frontier, *IDEA – The Law Review of the Franklin Pierce Center for Intellectual Property*, 2020, 60/1. szám, 145. o.

1. BEVEZETÉS

2022. szeptember közepén az iráni erkölcsrendészet – a hidzsáb nem megfelelő viselésére hivatkozva – letartóztatta Mahsza Aminit, aki a rendőrségen kómába esett, majd elhunyt. A történteknek az állami hivatalnokok és az iráni állampolgárok olvasatában két szöges ellentétben álló olvasata van, de az tény, hogy az országban három éve nem látható mértékű tiltakozási hullám indult el ennek következtében. Egyes források szerint már több mint kétszáz halálos áldozata van a megmozdulásoknak, és ezres nagyságrendű a sebesülések és letartóztatások száma.[5] Ám a kérdés nem csupán ezért érdekes: az iráni kormányzat ugyanis – Eisza Zarepur iráni távközlési miniszter tájékoztatása szerint – „biztonsági megfontolások miatt bizonyos korlátozásokat vezetett be".[6] És bár a miniszter még aznap cáfolta, hogy ilyet állított volna,[7] a kiberbiztonság és a digitális kormányzás nyomon követésével foglalkozó, saját magára csak az internet megfigyelőközpontjaként hivatkozó NetBlocks állítja, hogy „Iránban a 2019. novemberi mészárlás óta a legszigorúbb internetkorlátozások vannak érvényben".[8] Mindez együtt járt a mobilhálózatok nagy részének leállásával, regionálisan megfigyelhető internetelérési zavarokkal és bizonyos felületek (Instagram, WhatsApp) korlátozásaival. Mahsza Amini szülőtartományát, Kurdisztánt teljes egészében elvágták a nemzetközi internetforgalomtól.[9] Az iráni történések két egyszerre izgalmas, ugyanakkor borzongató gondolatkört is elénk tárnak: egyrészt egyre több ország kormánya használja a felmerülő problémák ideiglenes megoldására az állampolgárai közötti kapcsolatfelvétel nehezítésével járó internetkorlátozásokat, másrészt mindenhol ugyanolyan nehezen hihető (és egyre abszurdabb és homályosabb) indokokra hivatkozva teszik mindezt, amit talán még a kormányzatok sem hisznek el. Ez a kérdéskör a kibertér biztonságának e kötetben tárgyalt állami és jogi, politikai-társadalmi, valamint tág értelemben vett védelmi-biztonsági területeit egyaránt alapjaiban érintő jelenség.

[5] Farnaz Fassihi – Cora Engelbrecht: Tens of Thousands in Iran Mourn Mahsa Amini, Whose Death Set Off Protests. *The New York Times*, 2022. október 26., https://www.nytimes.com/2022/10/26/world/middleeast/iran-protests-40-days.html.

[6] N/A: Iran may disrupt internet for 'security reasons' as protests extend to day five. *Reuters*, 2022. szeptember 21., https://english.alarabiya.net/News/middle-east/2022/09/21/Iran-may-disrupt-internet-for-security-reasons-as-protests-extend-to-day-five.

[7] N/A: Iran minister says he was misquoted saying authorities might disrupt internet. *Reuters*, 2022. szeptember 21., https://www.reuters.com/world/middle-east/internet-may-be-disrupted-iran-security-reasons-2022-09-21/.

[8] https://twitter.com/netblocks/status/1572651793355603972.

[9] Sebastian Moss: Iran's Kurdish region hit by Internet blackout amid protests over death of Mahsa Amini. *DCD*, 2022. szeptember 20., https://www.datacenterdynamics.com/en/news/irans-kurdish-region-hit-by-internet-blackout-amid-protests-over-death-of-mahsa-amini/.

2. „A SZŰRÉS, A BLOKKOLÁS ÉS A HEKKELÉS VÁLTOTTA FEL AZ OLLÓT ÉS A FEKETE TINTÁT"[10]

Az ENSZ véleménynyilvánítás szabadságáért felelős különleges jelentéstevője már 2011-es jelentésében arról írt, hogy növekvő számban jelenik meg „néhány mód, ahogyan az államok egyre inkább cenzúrázzák az online információkat: a tartalmak önkényes blokkolása vagy szűrése, a jogos véleménynyilvánítás kriminalizációja, a közvetítő felelősségének megállapítása, a felhasználók lekapcsolása az internetről[11] (többek között a szellemi tulajdonról szóló törvények alapján), kibertámadások, valamint a magánélethez való jog és az adatok elégtelen védelme".[12] A jelentés az államok által alkalmazott, a tartalmak végfelhasználóhoz való eljutását megakadályozni hivatott különböző intézkedéseket és kísérleteket említ, így többek között az alábbiakat:

- felhasználók hozzáférésének megakadályozása bizonyos weboldalakhoz, IP-címekhez, valamint tartománynév-kiterjesztésekhez;
- weboldalak eltávolítása a gazdaszerverről;
- szűrőtechnológiák használata a meghatározott kulcskifejezéseket tartalmazó oldalak kizárására, illetve meghatározott tartalmak betöltésének megakadályozására.

Már a 2019-es internetleállításokról szóló 2020-as kiadású #KeepItOn jelentés is aggodalomra adott okot, amikor így fogalmazott: „A #KeepItOn koalíció 2019-ben a leállítások számának növekedését rögzítette,[13] valamint a fenntartott és hosszabb ideig tartó, továbbá célzott internetleállítások felé mutató trendet dokumentált."[14] Világszerte legalább 213 dokumentált leállítás történt 2019-ben, és az érintett országok száma a 2018-as 25-ről 33-ra nőtt. Ugyanezen szervezet legfrissebb, 2021-es kiadású jelentésében a korábbi évekhez képest csökkenő számokat találhat az olvasó,[15] ugyanakkor a jelentés egyértelművé teszi, hogy ennek legfőbb oka a Covid19 világ-

[10] Philip Bennett – Moises Naim: 21st-century censorship, *Columbia Journalism Review*, 2015, 14/1.

[11] Az első ismert internetleállítás 2007-ben történt a Guineai Köztársaságban. Scott Carpenter: The Internet Shutdowns Issue. *The Current*, 2021/4., https://jigsaw.google.com/the-current/shutdown/.

[12] UNHRC: *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,* 2011, UN Doc A/HRC/17/27, Összefoglaló.

[13] A dokumentum a leállítások széles körét monitorozza, így idetartoznak mind a mobilhálózatok, mind az internethálózatok – akár teljes, akár részleges – blokkolásával kapcsolatos esetek. A dokumentum így az IP-címek blokkolásával járó kérdéseket és a forgalomnak csupán a lassításával járó kormányzati lépéseket is a problémás esetek közé számítja.

[14] AccessNow: *Targeted, Cut off, and Left in the Dark,* 2020. február 24., https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf, 1. o.

[15] Dokumentált leállítások száma 2020-ban: 155, érintett országok száma 2020-ban: 29.

járvány és az azt követő fizikai lezárások lehetnek.[16] Ennek okán a jelentés igazából egy pillanaképet ábrázol csak, amely nem biztos, hogy a probléma valódi súlyát mutatja, ráadásul „a leállások kisebb száma nem jelzi a leállások hatásának csökkenését vagy a digitális jogok általános növekedését".[17]

A lista elején álló három ország 2019-ben India, Venezuela és Jemen, 2020-ban pedig India, Jemen és Etiópia. Kiemelésre méltó emellett, hogy az összes leállítás majdnem 20%-a egy hétnél is tovább tartott. Az adatokat tovább vizsgálva az is egyértelmű, hogy nem csak az autoriter rezsimek és a politikai változáson áteső országok korlátozták az internetet: Európa-szerte 2019-ben legalább öt, míg 2020-ban legalább három internetleállítás történt.[18]

Még akkor is, amikor egy állam nem volt képes arra, hogy saját földrajzi határain belül leállítsa az internetet, elérte nagyjából ugyanezt, csak más eszközökkel. Az egyik módszer a sávszélesség korlátozása, amely hatékonyan lassítja az internetes forgalmat *(throttling)*, míg más módszerek kizárólag a közösségimédia-oldalakat célozták, azonban mindkét módszer megzavarja az információ szabad áramlását. A leállítások, illetve lelassítások tényleges számát szinte lehetetlen pontosan meghatározni: gyakori eset, hogy az internetleállítással vádolt kormányzatok nem minden esetben ismerik el felelősségüket.[19] Amikor mégis, akkor a kormányzatok bevallott jogi céljai közé tartoztak „az álhírek, a gyűlöletbeszéd, valamint az erőszakra ösztönző tartalmak elleni küzdelem, a közbiztonság, a nemzetbiztonság, a harmadik felek tevékenységei és az iskolai vizsgák".[20] Az államok a műszaki problémák növekvő számát is felhozták kifogásként, habár sokan ezt az állítást vitatják, és úgy hiszik, a valódi okok máshol keresendők, hiszen a leállítások megszaporodnak politikai jellegű tiltakozások vagy erőszakos cselekmények idején ugyanúgy, mint amikor egy országban választásokat tartanak, vagy a politikai helyzet instabil. A 2020-as jelentés szerint úgy tűnik, hogy kivételes körülmények (pl. választások, katonai cselekmények, vallási ünnepek, kormánytisztviselők látogatásai) esetén az államok hajlamosak rendkívüli (nem szabályos) intézkedéseket alkalmazni a vélt vagy valós problémák nyílt kritizálásának megakadályozására. Az ilyen leállítások ráadásul

[16] AccessNow: *Shattered dreams and lost opportunities – a year in the fight to,* 2021a. március 3., https://www.accessnow.org/cms/assets/uploads/2021/03/KeepItOn-report-on-the-2020-data_Mar-2021_3.pdf, 2. o.

[17] AccessNow, 2020, 2. o.

[18] AccessNow, 2020, 3. o.; AccessNow, 2021a, 5. o.

[19] Ismeretesek olyan esetek is, amikor a kormányok jelentős nyomást gyakoroltak az online platformkora, hogy ne osszák meg nyilvánosan a meghozott intézkedésekre vonatkozó információkat. UNHRC: *Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights*, 2022, A/HRC/50/55, 30.

[20] AccessNow, 2020, 13. o.; AccessNow, 2021a, 10. o.

óhatatlanul sok jogszerű tevékenységet folytató felhasználót érintenek, ami a kormány által tervezett célokon túlmenően hatalmas járulékos károkat is tud okozni.[21]

Az internetleállítás ezenfelül is számos területen tud jelentős alapjogi problémákat okozni, elég csak a választásokra, az egészségügyre, az oktatásra vagy a közérdekű adatok elérésének kérdéseire gondolni. Az ENSZ emberi jogi főbiztosának 2022. évi legfrissebb jelentése így fogalmaz annak kapcsán, hogy milyen helyzetekben merülhetnek fel a kulcsfontosságú információk elérésével kapcsolatos működési zavarok: „A kórházak vészhelyzetben nem tudnak kapcsolatba lépni orvosaikkal, a választók nem kapnak információt a jelöltekről, a kézművesek nem tudnak kapcsolatba kerülni a vásárlóikkal, és potenciálisan a gazdasági csőd közelébe kerülnek, az erőszakos támadás áldozatául esett békés tüntetők nem tudnak segítséget kérni, a diákok lemaradnak a felvételi vizsgákról, a menekültek pedig nem tudnak hozzáférni a koronavírus (Covid-19) világjárvány miatt őket fenyegető kockázatokról – ez csak néhány olyan helyzet, amellyel az internet- és távközlési szolgáltatások leállása esetén szembesülni kell."[22]

3. AZ INTERNETELÉRÉS KORLÁTOZÁSA ÁLLAMI ESZKÖZÖKKEL AFGANISZTÁNTÓL UKRAJNÁIG

Az ENSZ véleménynyilvánítás szabadságáért felelős különleges jelentéstevője aggályát fejezte ki 2020-ban amiatt, hogy „a kormányzatok egyre gyakrabban folyamodnak az internet lekapcsolásához, gyakran jogtalan célokból, és a lakosságra nézve minden esetben aránytalan hatásokat okozva".[23] A szólásszabadság megvalósulása felől közelítve a kérdéshez, nehéz nem arra gondolni, hogy a nehéz politikai, gazdasági vagy társadalmi helyzetekben mennyire hasznos a lakosság számára az információk minél szélesebb köréhez való hozzáférés.

És az aggasztó tendencia folytatódik: hasonló technológiák, helyzetek és indoklások figyelhetők meg szerte a világban az elmúlt években, és a technikai adatok

[21] Ezzel kapcsolatban a nemzetközi bírósági gyakorlatból lásd *Ahmet Yildırım v. Turkey* App no. 3111/10 (ECtHR, 18 December 2012); *Cengiz and Others v. Turkey* App nos 48226/10 and 14027/11 (ECtHR, 1 December 2015); *Bulgakov v. Russia* App no. 20159/15 (ECtHR, 23 June 2020); *Engels v. Russia* App no. 61919/16 (ECtHR, 23 June 2020); *OOO Flavus and Others v. Russia* App nos 12468/15, 23489/15, and 19074/16 (ECtHR, 23 June 2020); *Vladimir Kharitonov v. Russia* App no. 10795/14 (ECtHR, 23 June 2020). Részletesen lásd Gosztonyi Gergely: *Cenzúra Arisztotelésztől a Facebookig.* Budapest, Gondolat Kiadó, 2022, 218–223. o.

[22] UNHRC, 2022, 1.

[23] UNHRC: *Disease pandemics and the freedom of opinion and expression,* 2020, UN Doc A/HRC/44/49, 25.

mindegyik esetben alátámasztották az állammal szembeni vádakat.[24] A hasonlóan csoportosítható esetek közé tartoznak például:

- A tálibok leállították az internetet Panjshir völgyében, ahol az (utolsó) ellenállók még kitartottak Afganisztánban;[25]
- A kormányzat korlátozta a Twittert Nigériában az elnök tweetjének törlése után;[26]
- A kormányellenes tüntetések közepette megszakadt az internet Kolumbiában;[27]
- Az indiai miniszterelnök látogatása elleni tüntetések közepette Bangladesben korlátozták a Facebookot;[28]
- Teljes internetleállítást figyeltek meg a Kongói Köztársaságban a választások napján;[29]
- Szenegálban a politikai zavargások közepette nem voltak használhatók a közösségimédia- és az üzenetküldő alkalmazások;[30]
- Csádban megszakadt az internetelérés az ellenzéki jelölt házánál tapasztalt halálos kimenetelű események után;[31]
- Ugandában a kormányzat döntése értelmében a választások estéjén vált elérhetetlenné az internethálózat;[32]

[24] A Witness Media Lab nem kormányzati szervezet (NGO) teljes útmutatót készített azzal kapcsolatban, hogy az internetleállításokat milyen technikákkal lehet offline módon is dokumentálni. http://lab.witness.org/projects/internet-shutdowns/.

[25] Ashraf Wani: Taliban shut down internet in Panjshir to prevent Amrullah Saleh from tweeting. *India Today*, 2021. augusztus 29., https://www.indiatoday.in/world/story/taliban-shut-down-internet-panjshir-amurullah-saleh-afghanistan-1846742-2021-08-29.

[26] John Campbell: Nigerian President Buhari Clashes With Twitter Chief Executive Dorsey. *Council on Foreign Relations Blog*, 2021. július 8., https://www.cfr.org/blog/nigerian-president-buhari-clashes-twitter-chief-executive-dorsey.

[27] Jon Jackson: Internet Disrupted in Colombia as Protesters Killed During Rally Against Iván Duque Márquez. *Newsweek*, 2021. május 5., https://www.newsweek.com/internet-problems-colombia-protests-1588991.

[28] N/A: Amid anti-Modi protests, Facebook says services restricted in Bangladesh. *CNA*, 2021. március 27., https://www.channelnewsasia.com/news/asia/anti-modi-protests-bangladesh-facebook-restricted-14505020.

[29] N/A: Internet shutdown in the Republic of the Congo on election day. *Digital Watch*, 2021. március 21., https://dig.watch/updates/internet-shutdown-republic-congo-election-day.

[30] Lawrence Agbo: #FreeSenegal: Senegal Disables Facebook, Other Social Media Apps. *Allnews Nigeria*, 2021. március 6., https://allnews.ng/news/freesenegal-senegal-disables-facebook-other-social-media-apps.

[31] N/A: Chad: Internet shutdowns impeding freedom of expression. *Amnesty International*, 2021. április 9., https://www.amnesty.org/en/latest/news/2021/04/tchad-les-coupures-internet-une-entrave-la-liberte-dexpression/.

[32] Carpenter, 2021.

- Örményországban a politikai zavargások és egy állítólagos puccskísérlet közepette megszakadt az internet;[33]
- Egész Mianmar területén nem működött az internet a katonai felkelés közepette;[34]
- A 2022-es tüntetések során egy teljes régió internet-hozzáférését állították le Iránban;[35]
- Az Ukrajna elleni teljes körű invázió kezdete óta az internet leállítása az orosz katonai stratégia részévé vált;[36]
- Kubában internet-összeomlást észleltek Los Palaciosban és Pinar del Rióban a kormányellenes tüntetések közepette.[37]

A sor hosszan folytatható: Brazília, Sierra Leone, Irak, Jemen vagy Szomália csak néhány ország a sok közül. A 2021-es #KeepItOn jelentés kiegészítése[38] ráadásul négy figyelemre méltó trendet is azonosított:

- az internetleállítások egyre hosszabb idejűek;
- választások alkalmával felerősödik ennek az eszköznek a használata;
- tüntetések alkalmával felerősödik ennek az eszköznek a használata; és
- aktív fegyveres konfliktusok alkalmával felerősödik ennek az eszköznek a használata.

Jól látható, hogy az internetes tartalmak politikai célú blokkolása a 2020-as években is a mindennapok része számos országban. A kínai internetszuverenitás a legszéleskörűbb megoldás, de 2021 nyarára felzárkózott Oroszország is: néhány évig próbálgatta a technológiát, végül 2021. június 15. és július 15. között – teszt jelleggel – sikeresen megvalósította az ország fizikai leválását a nemzetközi internethálózatról.[39] Minden-

[33] N/A: Internet disrupted in Armenia amid political turmoil and alleged coup attempt. *Digital Watch*, 2021. február 25., https://dig.watch/updates/internet-disrupted-armenia-amid-political-turmoil-and-alleged-coup-attempt.

[34] AccessNow: *Update: internet access, censorship, and the Myanmar coup,* 2021. február 15., https://www.accessnow.org/update-internet-access-censorship-myanmar/.

[35] Sharareh Abdolhoseinzadeh: International Consequences of Internet Restrictions in Iran. *Jurist*, 2022. december 24., https://www.jurist.org/commentary/2022/12/sharareh-abdolhoseinzadeh-iran-internet-censorship/.

[36] AccessNow: *#KeepItOn: Who is shutting down the internet in Ukraine?* 2022. december 15., https://www.accessnow.org/who-is-shutting-down-the-internet-in-ukraine/.

[37] David Belson: Internet disruptions overview for Q3 2022. *The Cloudfare Blog*, 2022. október 18., https://blog.cloudflare.com/q3-2022-internet-disruption-summary/.

[38] AccessNow: *#KeepItOn Update: Who is shutting down the internet in 2021?* 2021. június 7., https://www.accessnow.org/who-is-shutting-down-the-internet-in-2021/.

[39] Ashley Collman: Russia disconnected itself from the rest of the internet, a test of its new defense from cyber warfare, report says. *Insider*, 2021. július 23., https://www.businessinsider.com/russia-cuts-self-off-from-global-internet-tests-defenses-rbc-2021-7.

nek alapja, hogy Oroszország 2019-ben fogadta el és léptette hatályba a szuverén internetről szóló törvényt, amely alapján:

- az orosz internetszolgáltatóknak olyan eszközöket kötelező telepíteniük, amelyek mélységi tartalom-ellenőrzést[40] tesznek lehetővé, és lehetővé teszik a szolgáltatók és az állami szervek számára, hogy megtalálják a fenyegető tartalmak eredeti forrását, és szükség esetén blokkolják őket;
- az internetszolgáltatóknak az ország webes forgalmát és információit államilag ellenőrzött pontokon keresztül kell vezetniük;
- a kormánynak joga van arra, hogy vészhelyzet esetén fizikailag leválassza az orosz internetet a nemzetközi internethálózatról.

Ráadásul a fenyegető tartalmak homályos törvényi meghatározása miatt a hatóságok – az önkényesség veszélyét magában hordozó – feladata, hogy eldöntsék, melyik helyzet követel nyomon követést, átirányítást vagy blokkolást. „A folyamat nem átlátható és visszaélések tárháza lehet", állította 2019-ben a Human Rights Watch, megjegyezve, hogy a törvény elfogadása „rossz hír Oroszország számára, és veszélyes precedenst teremt más országok számára".[41]

A 2022-ben Ukrajna ellen indított brutális katonai agresszió[42] után az orosz helyzet csak romlott a korábbihoz képest.[43] Az orosz kormány elkezdte blokkolni és szélsőséges szervezetnek nyilvánítani azokat a nyugati platformokat (Twitter, Facebook, Instagram), amelyek az orosz lakosság számára a propagandahíreken kívül valódi információkkal tudtak volna szolgálni. Ezen platformok ráadásul az orosz bíróságok előtt jelentős összegű bírságokat is kaptak, mert megtagadták a felhasználóik azonosítását, illetve nem távolították el az orosz hatóságok szerinti „fake news" híreket az orosz–ukrán háború kapcsán.[44] A hatóságok olyan jogszabályokat is elfogadtak, amelyek „kibővítették az internet szabályozásával megbízott állami szervek

[40] Deep Packet Inspection (DPI). Kovács Zoltán 'mély csomagellenőrzésnek' nevezi: Kovács Zoltán: Biztonság vs. törvényes ellenőrzés az internet alapú kommunikációban – ellentétes vagy egymással megférő követelmények? I., *Hadmérnök*, 2016, 11/4., 134. o.

[41] Human Rights Watch: Russia: New Law Expands Government Control Online. *Wider Internet Surveillance,* 2019. október 31., https://www.hrw.org/news/2019/10/31/russia-new-law-expands-government-control-online.

[42] Kelemen Roland: Cyberfare state – Egy hibrid állammodell 21. századi születése. *Military and Intelligence CyberSecurity Research Paper*, 2022/1., 9. o.; Mart Susi – Wolfgang Benedek – Gregor Fischer-Lessiak – Matthias C. Kettemann – Brigit Schippers – Jukka Viljanen (szerk.): *Governing Information Flows During War: A Comparative Study of Content Governance and Media Policy Responses After Russia's Attack against Ukraine.* Hamburg, Verlag Hans-Bredow-Institut, 2022, GDHRNet Working Paper #4, 1–32. o.

[43] A 2022 előtti orosz folyamatokról részletesen lásd Gosztonyi, 2022, 229–230. o.

[44] N/A: Russia fines Google $370 million for repeated content violations, regulator says. *Reuters*, 2022. július 18., https://www.reuters.com/technology/google-is-fined-390-mln-russia-not-deleting-banned-content-interfax-2022-07-18/.

hatáskörét, valamint azt, hogy milyen tartalmak minősülhetnek illegálisnak".[45] Figyelemre méltó, hogy 2023 februárjában 1 331 276 szájt szerepelt egy civil szervezet, a RoskomSvoboda tiltott weboldalakat nyilvántartó regiszterében.[46]

A politikai tartalmak blokkolásának eminens tanulója immár évek óta a Kínai Népköztársaság. Sajtóbeszámolók megjegyezték, hogy a nagy kínai platformokon (WeChat, Weibo) a cenzorok szinte minden tartalmat moderálnak az orosz–ukrán háborúval kapcsolatban, akármelyik felet is támogatják.[47] A nyilvánosságtól elzárt tartalmak nagyon széles kört jelentenek ebben az esetben: a livefeedek, a hashtagek, a videók ugyanúgy a tiltott körbe tartoznak, mint a blogok vagy a közösségi médiás közlések.

Az ország számára a fő kérdés az internetszuverenitásról szól, amelynek alapja Hszi Csin-ping, a Kínai Népköztársaság elnökének 2015-ben, a második Internet Világkonferencia nevű rendezvényen elmondott beszéde, amelyben felszólította a világ országait, hogy tartsák tiszteletben egymás „kiberszuverenitását" és az internetes kormányzás különböző modelljeit.[48] Kiemelte, hogy a világ országainak joguk van megválasztani az internetük fejlesztésének és szabályozásának módját, és visszautasította, hogy a kibertérben bármely ország internethegemóniát szerezzen. 2020-ban a Freedom House éves internetről szóló jelentésében így fogalmazott: „Kína megfigyelési rendszerei továbbra is a legfejlettebbek és legszéleskörűbbek a világon."[49] A Nagy Kínai Tűzfal és az Arany Pajzs elemei ugyanis a 2020-as évekre már nem csupán az online aktivitásokat figyelik és cenzúrázzák szükség esetén, hanem olyan összekapcsolódó rendszert alkotnak, amely alapján a politikai és szociális profilozás könnyedén megvalósítható.[50] A 2022-es évben kiemelt figyelmet érdemelt, hogy a 2022-es pekingi olimpiával és a Covid19 világjárvánnyal kapcsolatos tartalmakat cenzúrázták[51], illetve szinte teljes körű tiltást vezettek be a VPN[52]-

[45] Freedom House: *Freedom on the Net 2022: Russia,* https://freedomhouse.org/country/russia/freedom-net/2022.

[46] https://reestr.rublacklist.net/ru/.

[47] Kai Wang: Ukraine: How China is censoring online discussion of the war. *BBC News*, 2022. március 12., https://www.bbc.com/news/60684682.

[48] Gosztonyi, Gergely: Special models of internet and content regulation in China and Russia. *ELTE Law Journal*, 2021/2., 95. o.

[49] Freedom House: *Freedom on the Net 2020. The Pandemic's Digital Shadow*, 2020. október 21., https://freedomhouse.org/sites/default/files/2020-10/10122020_FOTN2020_Complete_Report_FINAL.pdf, 21. o.

[50] Gosztonyi, 2021, 92–94. o.

[51] Helen Davidson: China brings in 'emergency' level censorship over zero-Covid protests. *The Guardian*, 2022. december 5., https://www.theguardian.com/world/2022/dec/02/china-brings-in-emergency-level-censorship-over-zero-covid-protests.

[52] Virtual Private Network: Zhensheng Zhang – Ya-Qin Zhang – Xiaowen Chu – Bo Li: An Overview of Virtual Private Network (VPN): IP VPN and Optical VPN. *Photonic Network Communications*, 2004, 7/3., 213–225. o.

használattal kapcsolatban. Emellett „előírták, hogy az online platformoknak »Hszi Csin-ping gondolatai«-hoz, azaz a hivatalos ideológiához kell igazítaniuk tartalommoderációs és ajánlási rendszereiket".[53] Emellett a GreatFire NGO adatai alapján a világ leglátogatottabb ezer weblapjából és közösségi média platformjából nagyjából kétszázat teljes mértékben tiltanak a Kínai Népköztársaságban.[54]

Mindkét országban külön érdekesség, hogy a kormányzatok sikerrel próbálják nem csupán a külföldi tartalmak elérését korlátozni, és a nemzetbiztonságra hivatkozva elzárni az állampolgárokat az életüket érintő fontos információktól, hanem a betiltott nyugati platformok helyére olyan hazai platformokat támogatnak, amelyekről okkal feltételezhetik, hogy a kormányzati álláspont akadálytalanul áramolhat rajtuk. Ilyen platformok Oroszországban a Vkontakte, amely a Facebook alternatívájaként működik, a Yandex a Google helyett, a RuTube a YouTube helyett vagy a Yappi a TikTok helyett. Ugyanezek Kínában a Weibo a Twitter vagy a WeChat a WhatsApp helyettesítőjeként, de Törökországban is megjelent a saját üzenetküldő/VoIP applikáció a WhatsApp helyett, amely BiP névre hallgat. Ezen alternatívákkal az autoriter jellegű kormányzatok az internetleállítások és applikációbetiltások után egy sokkal szorosabb ellenőrzést tudnak gyakorolni a felhasználók szólásszabadsága felett.

Az ENSZ véleménynyilvánítás szabadságáért felelős különleges jelentéstevője 2020-as jelentésében kiemelte, hogy „az internetleállítások sértik a véleménynyilvánítás szabadságát, amelyet minden embernek garantálnak az emberi jogok".[55] Ráadásul, ahogy Bennett és Naim megjegyzik: „az egyik nyugtalanító tendencia az, hogy a kormányok összefognak, hogy olyan internetet hozzanak létre, amelyet könnyebb monitorozni. Kína tanácsokkal látta el Iránt abban, hogyan építsen önálló »Halal« internetet. Peking ugyancsak megosztotta know-how-ját Zambiával, hogyan blokkolja a kritikus webes tartalmakat."[56]

Ugyanilyen figyelemfelhívó eredményre jutott Paul Bischoff is a vezetésével lefolytatott, 2023 elején publikált kutatás során.[57] A kutatók hat komponens kapcsán megvizsgálták, hogy (1) a torrentezés, (2) a pornográfia, (3) a hírmédia, (4) a közösségi média, (5) a VPN-ek és (6) az üzenetküldő/VoIP applikációk használata és elérhetősége szenved-e csorbát a világ országaiban: minden faktor esetében egy pontot jelentett, ha a szolgáltatások elérhetőek, de korlátozások alá esnek, míg két pontot,

[53] Freedom House, 2022, 9. o.

[54] https://en.greatfire.org/search/alexa-top-1000-domains.

[55] UNHRC, 2020, 28.

[56] Bennett–Naim, 2015. Vö.: „Szükséges lenne a cenzúra és a megfigyelési technológia exportjának korlátozása." Freedom House: *Freedom on the Net 2021. The Global Drive to Control Big Tech*, 2021. szeptember 16., https://freedomhouse.org/sites/default/files/2021-09/FOTN_2021_Complete_Booklet_09162021_FINAL_UPDATED.pdf, 25. o.

[57] Paul Bischoff: Internet Censorship 2023: A Global Map of Internet Restrictions, *comparitech.com*, 2023, https://www.comparitech.com/blog/vpn-privacy/internet-censorship-map/.

ha teljes mértékben le vannak tiltva. Ebből következően minél magasabbak egy ország összpontszámai, annál nagyobb fokú ott a cenzúra és a tartalmak korlátozása. A kutatásból kitetszik, hogy a probléma jelentős számú országot érint a világon: a legmagasabb pontszámokat Kína, Észak-Korea, Irán, Mianmar, Türkmenisztán és az Egyesült Arab Emírségek kapták.[58]

És mielőtt Európában arra gondolnánk, hogy ez a világ többi részének problémája, Bischoff és társai 2023 elején megjegyezték, hogy a helyzet Európában sem tökéletes, ugyanis majdnem minden európai ország használ eszközöket a szólásszabadság és a tartalmakhoz való hozzáférés korlátozására. Ahogy Európával kapcsolatban megjegyzik: 18 országban tiltják részlegesen vagy teljesen a torrent használatát, több országban pedig a jogi hátteret alkották meg ehhez. Emellett négy országban (Fehéroroszország, Spanyolország, Törökország, Ukrajna) korlátozzák a közösségi média elérését, két helyen pedig a VPN-használatot. Fehéroroszország és Törökország szigorúan cenzúrázza a politikai jellegű médiatartalmakat, de 12 másik európai országban is találtak a kutatók korlátozásra utaló jeleket. Vint Cerf, az internet egyik atyja így foglalta ezt össze: „Egyes tekintélyelvű kormányok számára az internet szabadsága fenyegetést jelent, és az online világ veszélyei ürügyet szolgáltatnak az internethasználók túlzott ellenőrzésére és a tartalom cenzúrázására. Az online szolgáltatások használatának kockázatai azonban még a demokratikus országokban is arra ösztönöztek, hogy a közösségi médiaszolgáltatókra, a webes keresőszolgáltatásokra, sőt az általános internet-hozzáférési szolgáltatókra is tartalomszabályozást vezessenek be."[59]

4. A 'SZILÁNKOS INTERNET' VESZÉLYE

2023 elején úgy tűnik, hogy egyre több ország kormányzata hisz az internetszuverenitás elméletében, amely egyre inkább a globális, nyitott és átjárható internet koncepciója ellen dolgozik. Az ezzel szemben álló 'szilánkos internet'[60] terjedése kapcsán megfigyelhető, hogy A) egyre több állam ellenőrzi az internetes infrastruktúrát, és használ (sokszor jogellenes módon) internetleállításokat, B) ezzel korlátozva az információk szabad áramlását, és C) a felhasználói adatok határokon átnyúló továbbítását. Ezen államok egyértelműen az állami hírek elsődlegességét hirdetik, amely együtt jár a független sajtó, az alternatív típusú médiumok és a civil társadalom jelentőségének tudatos visszaszorításával.[61]

[58] Uo.

[59] Cerf Vint: Censoring the net is not the answer, but... *Index on Censorship*, 2022, 51/1., 51. o.

[60] Az angol szakkifejezés (splinternet) a splinter (szilánk) és az internet összekapcsolásából ered.

[61] Gosztonyi Gergely: *Alternatív (?) média. A közösségi média jogi szabályozásának vetületei.* Budapest, Eötvös Kiadó, 2014.

Az internetleállítások és -korlátozások azonban egy nagyobb hatalmi játszma részei, amelynek az alapkérdése úgy hangzik, hogy ki fogja meghatározni ennek a kommunikációs térnek a játékszabályait. Hosszú éveken keresztül megfelelt az államoknak a véleménynyilvánítás „privatizációja"[62], mígnem először Kína, majd Oroszország olyan utat választott, amely az online világ kormányzójaként fellépő Amerikai Egyesült Államoknak (USA) nem volt ínyére. A szavak szintjén a nagy szereplők egyetértenek abban, hogy valamiféle nemzetközi szabályozási kódexre lenne szükség, ám a javasolt megoldások kapcsán az álláspontok nem is lehetnének messzebb egymástól.

Orosz diplomaták a Nemzetközi Távközlési Uniót[63] kívánnák valamiféle nemzetközi szabályozó szervvé alakítani. Az ötletet támogatta Észak-Korea, Fehéroroszország, Kambodzsa, Kína, Mianmar, Nicaragua és Venezuela is,[64] azaz olyan országok, ahol a demokrácia megvalósulása legalábbis kérdéses. Magas rangú orosz és kínai vezetők továbbra is az internetszuverenitás kérdését tartják alapvetőnek a nemzetközi szabályozás megalkotásakor, azaz a szavak és a valódi szándékok jelentősen eltérnek egymástól. Ráadásul Szergej Viktorovics Lavrov orosz külügyminiszter 2022-ben úgy nyilatkozott, hogy „A világot a kiberanarchia veszélye fenyegeti, hacsak nem dolgozunk ki és fogadunk el egy egyetemes magatartási kódexet".[65] Enélkül katasztrofális következményekre hívta fel a figyelmet, és kiemelte, hogy eltökélt szándékuk, hogy az internet szabályozásának „igazságosabb és kiegyensúlyozottabb nemzetközi rendszerét szorgalmazzuk".[66] Nem nehéz kiolvasni ebből, hogy melyik ország a nyilatkozat valódi címzettje…

Az USA – válaszképpen a fentiekre és az orosz–ukrán háború eseményeire – politikai nyilatkozatot[67] fogadott el az Európai Unióval (EU) és (immár) 61 aláíró állammal egyetemben[68] a növekvő digitális tekintélyelvűség (azaz a fent vizsgált kiberszuverenitás elmélete) ellen.[69] A nyilatkozat aláírói kijelentik, hogy az internetnek „nyitottnak, ingyenesnek, globálisnak, interoperábilisnak, megbízhatónak és biztonságosnak

[62] Arne Hintz: Social media censorship, privatized regulation, and new restrictions to protest and dissent. In Lina Dencik – Oliver Leistert (szerk.): *Critical Perspectives on Social Media and Protest: Between Control and Emancipation*. London, Rowman & Littlefield, 2015, 111. o.

[63] International Telecommunication Union (ITU).

[64] Freedom House, 2022, 17. o.

[65] TASS: *Without code of conduct in Internet sphere world will plunge into cyberanarchy – Lavrov*, 2022. április 14., https://tass.com/politics/1437587.

[66] Uo.

[67] Nyilatkozat az internet jövőjéről (A declaration for the future of the Internet), https://www.whitehouse.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet_Launch-Event-Signing-Version_FINAL.pdf.

[68] A nyilatkozatot Magyarország is aláírta.

[69] Pozitívum, hogy a 2022-ben elfogadott nyilatkozat már egy jelentősen módosított változata a 2021-es tervezetnek, amely túlzottan az USA gazdasági és politikai érdekeire fókuszált. A tervezet szövegét lásd: https://www.politico.com/f/?id=0000017c-e71b-d8e1-a57c-efffa3810004.

kell lennie".[70] Mindennek megtartására az aláírók törekszenek az egyetemes internethozzáférés előmozdítására, az emberi jogok védelmére, a tisztességes gazdasági verseny biztosítására, a biztonságos digitális infrastruktúra kialakítására, a pluralizmus és a szólásszabadság előmozdítására, valamint az internet irányításának többszereplős megközelítésére. Kiemelik, hogy a demokratikus államokban elfogadhatatlan az internetleállítások gyakorlata ugyanúgy, mint az államilag terjesztett propaganda. A nyilatkozat felhívja a világ államainak figyelmét, hogy tartózkodjanak a kormányok által elrendelt (akár teljes, akár részleges) internetleállításoktól ugyanúgy, mint a jogszerű tartalmakhoz, szolgáltatásokhoz és alkalmazásokhoz való hozzáférés blokkolásától. A kritikusok ugyanakkor „fölöslegesnek és zavarónak"[71] minősítették a nyilatkozatot, amelynek nincs jogi kötőereje, és amihez semmiféle kikényszerítő mechanizmus nem párosul.[72] A nyilatkozat célja talán nem is Kína, Oroszország vagy Irán meggyőzése,[73] hogy ne a digitális autoritarianizmus eszméit kövessék, hanem „meggyőzni számos kevésbé elnyomó államot arról, hogy a nyitott internet az ő érdekükben áll".[74]

5. KONKLÚZIÓ

Az ENSZ Emberi Jogi Tanácsa már 2016-ban kimondta, hogy „ahhoz, hogy az internet globális, nyitott és átjárható maradjon, elengedhetetlen, hogy az államok a saját nemzetközi emberi jogi kötelezettségeiknek – különös tekintettel a véleménynyilvánítás szabadságára, az egyesülés szabadságára és az adatvédelemre – megfelelve kezeljék a biztonsági aggályokat".[75] Hat évvel később, 2022 közepén az ENSZ emberi jogi főbiztosának mégis újra ki kellett nyilvánítania, hogy az internetleállítások kérdéskörre még mindig jelentősen alul van értékelve, hiszen jól látható, hogy az államok „túl gyakran lassítják vagy blokkolják a főbb kommunikációs csatornákat vagy egész kommunikációs hálózatokat, néha hivatalos elismerés vagy indoklás nélkül, megfosztva ezzel ezreket vagy akár milliókat az egyetlen lehetőségüktől, hogy elérjék szeretteiket, folytassák munkájukat vagy részt vegyenek a politikai vitákban vagy döntéshozatalban".[76] A Surfshark 2022-es jelentése alapján az internetkorlátozások 1,9 milliárd em-

[70] Nyilatkozat az internet jövőjéről.

[71] AccessNow: *Empty promises? Declaration for Future of the Internet is nice on paper.* 2022. április 28., https://www.accessnow.org/declaration-for-future-internet/.

[72] Hasonló politikai nyilatkozatot kezdeményezett a dán kormányzat is 2021-ben, The Copenhagen Pledge on Tech for Democracy néven: https://techfordemocracy.dk/join-the-initiative/.

[73] Ahogy a nyilatkozat is fogalmaz: „Ezek az alapelveknek jogilag nincs kötelező erejük, hanem inkább referenciaként szolgálnak a politikai döntéshozók, valamint az állampolgárok, a vállalkozások és a civil szervezetek számára."

[74] Freedom House, 2022, 4. o.

[75] UNHRC: *The Promotion, Protection and Enjoyment of Human Rights on the Internet*, 2016, UN Doc A/HRC/32/L.20.

[76] UNHRC, 2022, 58.

bert érintettek 2022 első felében,[77] míg a Top10VPN arra hívja fel a figyelmet, hogy az amúgy is számos sokkhatástól szenvedő világgazdaságnak a leállítások csak 2022-ben 24 milliárd dollárba kerültek.[78] Az ENSZ emberi jogi főbiztosa kiemelte, hogy az emberi jogokra gyakorolt megkülönböztetés nélküli és aránytalan hatásukra, az államoknak tartózkodniuk kellene az internet teljes körű leállításától.[79]

Mindezek alapján 2023-ban érezhető és látható, amit Romain Badouard úgy fogalmazott meg, hogy „ma egy demokratikus paradoxonnal állunk szemben. Sok szempontból a véleménynyilvánítás szabadságának aranykorát éljük, mivel soha nem volt még ilyen könnyű nyilvánosságra hozni egy gondolatot, és azt lehető legtöbb emberhez eljuttatni. Ugyanakkor soha nem volt még ilyen könnyű korlátozni, szűrni és blokkolni a beszédet, és a beszéd megakadályozása még soha nem összpontosult ilyen kevés magánszereplő kezében."[80]

A globális, nyitott és átjárható internet mítoszára sajnos jelentősen rácáfol az a tény, hogy a világ lakosságának majdnem 40%-a számára a szabad és korlátozásoktól mentes internetelérés, így a szólásszabadság érvényesülése csupán vágyálom.[81] Tekintettel azonban arra, hogy az internet olyan sok ember számára vált az emberi jogok gyakorlásának és kifejezésének, az információk és az ötletek fogadásának és átadásának, valamint az államok és a csoportok marginalizációja elleni küzdelemnek az eszközévé a különböző társadalmakban,[82] a korlátozást jelentő esetek növekvő száma világos figyelmeztetés. Mind egy nemzet demokratikus működése és biztonsága, mind a szólásszabadság kapcsán létfontosságú, hogy az államok ne lökjék saját állampolgáraikat a digitális sötétségbe.[83]

[77] Varun Aggarwal: Government-imposed internet shutdowns impacted 1.9 billion people in first half of 2022. *Network World*, 2022. augusztus 4., https://www.networkworld.com/article/3669388/government-imposed-internet-shutdowns-impacted-19-billion-people-in-first-half-of-2022.html. Vö.: UNHRC, 2022, 33–34.

[78] Samuel Woodhams – Simon Migliano: Government Internet Shutdowns Cost Almost $24 Billion in 2022. *Top10VPN*, 2023. január 3., https://www.top10vpn.com/research/cost-of-internet-shutdowns/.

[79] UNHRC, 2022, 66.

[80] Badouard, 2020, 11–12. o.

[81] Freedom House, 2022, 5. o.

[82] *Cengiz and Others v. Turkey* App nos 48226/10 and 14027/11 (ECtHR, 1 December 2015), [49.].

[83] Jain Shilpa – Variath Adithya: Internet Shutdowns and Virtual Curfews: Searching for Rights in Digital Darkness. *Journal on Human Rights Practice*, 2020, 4/2., 35–48. o.

KÁDÁR PÁL

A kibertér és a kibertérműveleti képességek jelentősége a védelmi és biztonsági tevékenységek összehangolásának fejlesztésében

1. A VÉDELMI ÉS BIZTONSÁGI SZABÁLYOZÁSI REFORM ÉS A KIBERMŰVELETEK ÖSSZEFÜGGÉSEI

A kibertér és a kibertérműveletek szerepe a 21. századi technológiai fejlődés folyamatos gyorsulásának, a digitalizáció soha nem látott térnyerésének és a kibertéren keresztül elérhető biztonsági helyzetet érintő információszerzés, befolyásolás, működés blokkolás vagy rombolás lehetőségének köszönhetően folyamatosan felértékelődik. Mindeközben a technológiai fejlődés üteme világszerte komoly kihívás elé állítja a jogalkotást, folyamatos kérdés, hogy miként lehet ezzel lépést tartani, jogállami, alkotmányossági szempontból és nemzetközi jogilag is megfelelő mederben tartani az ezzel összefüggésben elengedhetetlen jogi felhatalmazások és eljárási szabályozások rendszerét. Merül fel ez úgy, hogy jelen kötet többi fejezete alapján is mondható, az információs korszak a politikai-társadalmi keretek és működés terén is érezhetően jelentős változásokat sejtet.

A hazai védelmi és biztonsági szabályozásban a 2020-as évek elejére már számos olyan elavult vagy az új kihívások[1] terén kevéssé alkalmazható elem szerepelt, amelyek korrekciója nélkül a jövőben a tényleges védekezés lehetősége beszűkült volna, egyes esetekben pedig – a nem megfelelő alkotmányos keretek miatt – akár el is lehetetlenedett volna a jogállami fellépés a biztonság megőrzése vagy helyreállítása érdekében.[2]

[1] Lásd erről Szenes Zoltán: Katonai biztonság napjainkban. Új fenyegetések, új háborúk, új elméletek. In Finiszter Géza – Sabjanics István (szerk.): *Biztonsági kihívások a 21. században.* Budapest, Dialog Campus, 2017, 69–101. o., Rada Péter: Átalakuló biztonsági kihívások. A biztonság dimenziói. *Grotius*, 2007 (Rada P\351ter \301talakul\363 biztons\341gpolitikai kih\355v\341sok.doc) (grotius.hu).

[2] A védelmi szabályozás reformjáról lásd bővebben Farkas Ádám: Szemléletváltást védelmi aspektusban! *Pázmány Law Working Papers*, 2015/18. szám; Kádár Pál: A védelmi-biztonsági szabályozás reformjának egyes kérdései az Alaptörvényen túl. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok.* 2021/11. szám.

A szürke zónás fenyegetések[3], a hibrid hadviselés[4], a kibertér kihívásai, a technológiai fejlődésből, a korlátok és ellenőrzés nélküli globális hálózatok[5] erősödéséből következő biztonsági kockázatok elegye a már ismert hagyományos kihívásokkal olyan kihívás elé állítja a védelmi és biztonsági szabályozási rendszereket szerte a világon, amelyre rendkívül nehéz megfelelően gyorsan és hatékonyan választ találni.[6] A hazai rendszer szabályainak alkalmazása egyes esetekben meglehetősen elavult lenne a felgyorsult világban, számos intézmény és beavatkozási lehetőség mára kiürült, értelmét vesztett, meghaladottá vált,[7] így ezek felülvizsgálatának elmaradása biztonsági kockázatot eredményezett volna. A megváltozott biztonsági környezet azonban önmagában nem jelentett volna beavatkozási kényszert, hiszen az évtizedeken át lényegében azonos alapon nyugvó szabályrendszerünk jó néhány új kihívást képes volt kezelni, kisebb jogi korrekciókkal[8] alkalmazkodva a helyzethez. A 2020-as évek elejére azonban olyan szinten korszerűtlenné vált a szabályozásunk,[9] amely már biztonsági kockázatként is értékelhetővé vált. A nem megfelelő

[3] Lásd erről Clementine G. Starling: What exactly is a "gray zone," and how has this concept developed in a post-Cold War world? *Atlantic Council,* 2022. 02. 23. (https://tinyurl.com/2s37smh5).

David Carment – Dani Belo: *War's Future: The Risks and Rewards of Grey Zone Conflict and Hybrid Warfare.* Calgary, Canadian Global Affairs Institiute, 2018.

[4] Bővebben: Frank G. Hoffman: Hybrid Warfare and Challenges. *Joint Force Quarterly,* 2009/1st quarter, 34–39. o.; Erik Reichborn-Kjennerud – Patrick Cullen: What is Hybrid Warfare? *Policy Brief,* 2016/1. szám; 1–4. o.; Bastian Giegreich: Hybrid Warfare and the Changing Character of Conflict. *The Quarterly Journal,* 2016/2. szám; 65–72. o.

[5] Bővebben: Barry Wellmann: The Network Community – An Introduction. In Barry Wellmann (szerk.): *Networks in the Global Village.* New York, Routledge, 2009, 7–54. o.

[6] A pandémai kapcsán elvégzett kutatás eredményei ezt az állításunkat egyértelműen alátámasztják. Gyakorlatilag 20 ország gyakorlatának és jogrendszerének vizsgálata nyomán bebizonyosodott, hogy egy nem várt, de lényegében egyszerű humánvírus okozta pandémia kezelésére sem voltak felkészülve a szabályrendszerek, a nemzetközi szervezetek együttműködése is nehezen valósult meg, szinte kivétel nélkül sajátos jogalkotásra volt szükség az egyes államokban. Lásd erről Nagy Zoltán – Horváth Attila (szerk.): *A különleges jogrend és nemzeti szabályozási modelljei.* Budapest, Mádl Ferenc Összehasonlító Jogi Intézet, 2021.

Valószínűsíthető, hogy egy összetettebb kihívás kezelése hasonló akadályokba ütközne, kiváltképp, ha a kialakult konfliktusban ellenérdekelt felekként jelennének meg az egyes államok.

[7] A 2011. évi CXIII. törvény 68. § (6) bekezdése értelmében rendkívüli állapotban és szükségállapotban „a nyomdák és más sokszorosításra alkalmas eszközök üzemeltetői szigorított biztonsági rendszabályok bevezetésére és megtartására kötelezhetők". Ennek a rendelkezésnek semmilyen gyakorlati haszna nincs egy olyan világban, ahol az internetes hálózatokon keresztül azonnal terjeszthető bármilyen információ, illetve ahol bármely háztartás képes lehet akár tízezres példányszámban röplapot nyomtatni.

[8] Ezek a kisebb korrekciók számos esetben akár alkotmánymódosítást is jelentettek, amely azonban a szabályozás magas jogforrási hierarchiai szintjére figyelemmel sem jelentett minden esetben mélyreható és rendszerszerű változást.

[9] Lásd erről Farkas: i. m. (2015). Hoffman István – Kádár Pál: A különleges jogrend és a válságkezelés közigazgatási jogi kihívásai. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* 2021/2. szám, 16–26. o.

szakmai kereteket biztosító alkotmányos szintű megközelítés olyan veszélyeket rejt magában, hogy a jogi keretek miatt akkor sem lenne lehetséges a fenyegetés elhárítása és a védekezés megszervezése, ha egyébként erre az állam eszközrendszerében rendelkezésre állnának a humánoldali és technikai feltételek.[10] A válságkezelés és a különleges jogrendi működés szabályozásának alkotmányos szintű korszerűtlensége determinálja az alacsonyabb szintű szabályok megközelítését is, lényegében a saját jogrendszerünk válhat az állam védelmi mechanizmusainak akadályává. Szélsőséges esetben ez olyan helyzetet is előidézhet, amely közvetlenül bénítja meg az állami szervek működését, jogi felhatalmazás hiányában lehetetlenné teszi a védekezést, amelyet az ellenérdekelt fél könnyűszerrel használhat akár egy fegyveres támadással egyenértékű hátrány okozására, melynek mára már egyre szélesebb irodalma is van.[11] A kibertér kihívásai mára a korábban széles körben elemzett kihívásokon túl messze túlmutatnak, a globális biztonságra gyakorolt hatásai egyre nagyobb hangsúlyt kapnak.[12]

A védelmi és biztonsági reform első, szabályozásban is beazonosítható eleme az Alaptörvény kilencedik módosítása volt, melyet 2020. december 15-ei ülésnapján fogadott el az Országgyűlés, azzal, hogy a különleges jogrendi szabályrendszerre vonatkozó rendelkezések 2023. július 1-én lépnek hatályba.[13]

Maga a különleges jogrendi szabályrendszert érintő reform egyik mozgatórugója éppen a kibertérben jelentkező kihívások kezelhetőségének megoldása volt. Ha az Alaptörvény 2022. november 1-jét megelőző szövegét vizsgáljuk, egyáltalán nem találunk a kibertérben jelentkező fenyegetések kezelésére konkrét felhatalmazást vagy utalást. Itt kell elmondanunk, hogy az Észak-atlanti Szerződés Szervezete is valami-

[10] Példaként hozható fel itt a katonai kibertérműveleti erők alkalmazásának szabályozása a Hvt. 62/A. §-ában, amelyre a tételes jog csak 2020. január 1. óta biztosít lehetőséget.

[11] Lásd Petruska Ferenc: Lawfare a védelmi szférában. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok*, 2022/18. szám, 1–16. o.; F. Kittrie Orde: *Lawfare: law as a weapon of war.* Oxford, New York, Oxford University Press, 2016; Jones Craig A.: Lawfare and the Juridification of Late Modern War. *Progress in Human Geography,* 2016/2. 221–239. o.; Kate Jean Dent: Lawfare and Legitimacy: *The Wicked Problem of Judicial Resilience at a Time of Judicialisation of Politics in South Africa (doctoral dissertation).* Cape Town, University of Cape Town, Faculty of Law, 2021. (https://open.uct.ac.za/handle/11427/35641.); Charles Dunlap Jr.: Lawfare 101 – A Primer. *Military Review*, 2017/May-June, 8–17. o.

[12] Hajdu Péter: A kibertér etikai, jogi és társadalmi kihívásai. *Új Pedagógiai Szemle,* 2001/7–8. szám; Munk Sándor: A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései. *Hadtudomány*, 2018/1. szám, 113–131. o.; Berzsenyi Dániel: Globális kihívás, regionális válaszok: kiberbiztonság Kelet-Közép-Európában. *Nemzet és Biztonság*, 2017/3. szám, 69–79. o.; David A Graham: Cyber Threats and the Law of War. *Journal of National Security Law & Policy*, 20101. szám, 87–102. o.; Haig Zsolt – Kovács László: Fenyegetések a cybertérből. *Nemzet és Biztonság*, 2008/5. szám, 61–69. o.

[13] A hatálybalépés időpontját az Alaptörvény tizedik módosítása 2022. november 1-ére módosította, egyidejűleg a veszélyhelyzetre vonatkozó rendelkezések szakmai tartalmát kiterjesztette a „szomszédos országban fennálló fegyveres konfliktus, háborús helyzet vagy humanitárius katasztrófa" esetkörére is.

féle kiterjesztő értelmezéssel operál, a kiberteret a varsói csúcs, 2016 óta műveleti domainként kezeli,[14] ami leegyszerűsítve azt jelenti, hogy a kibertérben érkező támadások vagy az ott folytatott műveletek lehetnek alapjai akár egy 5. cikk[15] szerinti műveletnek is. Ezt a megoldást kellett volna választania a hazai jogalkalmazóknak is adott esetben, mindaddig, amíg a védelmi és biztonsági tevékenységek szabályozási reformjának elemei hatályba nem lépnek. A reform szabályrendszere a jövőre nézve e vonatkozásban ugyan szintén nem tartalmaz konkrét alaptörvényi szintű rendelkezést, azonban a különleges jogrendi tényállások fogalmi pontosítása és profiltisztítása eredményeként olyan rugalmas esetkörök kerültek a szabályozásba, amelyek alapján már nem okozhat gondot az alacsonyabb szintű szabályok megalkotása vagy akár a tényleges kiberműveletek végrehajtása sem.

Nem szabad azt sem figyelmen kívül hagynunk, hogy a fenyegetettségi mátrix napjainkban jellemzően rendkívül összetett, amelyen belül alacsony a valószínűsége a kizárólag kibertéren át és kizárólag informatikai hatásokat célzó módon végrehajtott műveleteknek, ezek rendszerint a hibrid műveletek részeként, információs műveletekkel kombinálva jelennek meg,[16] és elsődleges céljuk nem az információtechnológiai eszközök működésének befolyásolása, hanem az ezeken keresztül elérhető további hatások generálása, melyek már az energiahálózatot, a kommunikációs infrastruktúrát, az ellátási láncokat üzemeltető berendezéseket, a pénzügyi rendszert, a médiát és végső soron az államszervezet egészének működését is képesek lehetnek megbénítani. Erre figyelemmel a jogi alapvetéseknek, az egyes felhatalmazásoknak mindezeket a szempontokat szem előtt tartva kell megszületniük, és az alacsonyabb szintű törvényi és rendeleti szabályokat ennek megfelelően kellett és kell a jövőben is alakítani.

[14] Lásd: NATO Cyber Defence factsheet (2008-factsheet-cyber-defence-en.pdf (nato.int); és NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit (https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/).

[15] The North Atlantic Treaty „Article 5 The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all; and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defense recognized by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area…".

[16] Lásd bővebben Damjan Štrucl: NATO in Cyber Domain című előadását; Tallin 2021 (https://www.researchgate.net/publication/350399333_NATO_in_Cyber_Domain).

2. AZ ALAPTÖRVÉNY KÜLÖNLEGES JOGRENDI RENDELKEZÉSEI ÉS A KIBERTÉR KIHÍVÁSAI

Az Alaptörvény kilencedik módosítása egyszerűsítette és egyben lényegesen rugalmasabbá tette az egyes különleges jogrendi esetek szabályrendszerét. Vizsgálatunk szempontjából elsőként a hadiállapot szövegezését érdemes górcső alá vennünk.

„49. cikk (1) Az Országgyűlés

a) háborús helyzet kinyilvánítása vagy háborús veszély,

b) külső fegyveres támadás, hatásában külső fegyveres támadással egyenértékű cselekmény, valamint ezek közvetlen veszélye, vagy

c) kollektív védelemre irányuló szövetségesi kötelezettség teljesítése

esetén hadiállapotot hirdethet ki."

A hadiállapot mint különleges jogrend a korábbi terminológiában a rendkívüli állapotnak feleltethető meg azzal az eltéréssel, hogy a rendkívüli intézkedések meghozatalára vonatkozó felhatalmazás az új rend szerint nem a Honvédelmi Tanácsot, hanem a Kormányt illeti, azaz a végrehajtó hatalom jogosult meghozni mindazon törvényektől eltérő intézkedéseket, amelyekkel a védekezés érdemben megvalósítható. Lényeges új szabály a 49. cikk (1) bekezdés b) pontjában szereplő „hatásában külső fegyveres támadással egyenértékű cselekmény" fordulat, amely valamennyi olyan cselekményt magában foglal, amely nem tényleges fegyveres támadásként jelentkezik. Ebbe a körbe sorolhatjuk a kibertérből – de nem csak onnan[17] – érkező támadásokat is. A jogszabályhely második fordulata azonban még ennél is tovább megy, hiszen az „ezek közvetlen veszélye" már olyan tág spektrumot ölel fel, amely a mindenkori kormányzat mérlegelésétől teszi függővé a beavatkozást. Közbevetőleg itt emelendő ki, hogy bár a hadiállapot kihirdetése az Országgyűlés kizárólagos jogosítványa, amelyhez a képviselők kétharmadának támogatása szükséges, hasonlóan a korábbi szabályozáshoz, azonban az Alaptörvény új szabálya lehetővé teszi a Kormány számára, hogy egyes rendkívüli intézkedéseket már a kihirdetés kezdeményezésekor megtehessen,[18] ezzel jelentősen túllépve az eddigi kereteken. Jogászi megközelítésben vizsgálva ezt a kérdést, a kibertámadások kapcsán meglehetősen nehéz megfogalmazni, mit is jelent egy „kibertámadás közvetlen veszélye". Amennyiben a technikai képesség kialakítását vagy a rosszindulatú kód előállítását ennek tekintenénk, gyakorlatilag folyamatosan hadiállapotban kellene lennünk. Vélhetőleg a gyakorlat majd segít kimunkálni ennek részleteit, amely nagy valószínűség-

[17] Példaként: az ivóvízbázis szándékos mérgezése vagy ipari katasztrófa szándékos előidézése is ebbe a körbe tartozóként kezelendő.

[18] Alaptörvény 54. cikk (1) Hadiállapot vagy szükségállapot kihirdetésének Kormány általi kezdeményezését követően a Kormány rendeletet alkothat, amellyel – sarkalatos törvényben meghatározottak szerint – a kihirdetésre okot adó körülmény azonnali kezeléséhez szükséges mértékben egyes törvények alkalmazását felfüggesztheti, törvényi rendelkezésektől eltérhet, valamint egyéb rendkívüli intézkedéseket hozhat *(Az Alaptörvény kilencedik módosításának megfelelő szövegváltozat).*

gel a szintén alkotmányos követelményként alkalmazandó szükségesség-arányosság tesztjével, illetve a fokozatosság elvének érvényesítésével tartható majd észszerű mederben.

Az Alaptörvény szintjén dolgozatunk szempontjából releváns következő elem a szükségállapot szabályozása:

„50. cikk (1) Az Országgyűlés

a) az alkotmányos rend megdöntésére, felforgatására vagy a hatalom kizárólagos megszerzésére irányuló cselekmény, vagy

b) az élet- és vagyonbiztonságot tömeges mértékben veszélyeztető súlyos, jogellenes cselekmény esetén szükségállapotot hirdethet ki."

E rendelkezést összevetve a korábban hatályos[19] szükségállapoti fogalommal szembeötlő, hogy a védelmi és biztonsági szabályozási reform e vonatkozásban is lényegesen rugalmasabb, tágabb esetkört érintően teszi felhívhatóvá ezt a klauzulát. Azzal a korrekcióval, amely szerint a jövőben nem szükséges a súlyosan jogellenes cselekménynek fegyveresen vagy felfegyverkezve elkövetettnek lennie, lényegében lehetséges szükségállapoti esetkörré tette a kibertámadások egyes eseteit is. A szükségállapoti szabályok alkalmazásának a rendszerváltást követő időszakban Magyarországon nincs hazai gyakorlati tapasztalata – ahogy a hadiállapotnak sem, szerencsére – de az elmondható, hogy egy ilyen szcenário modellezése legalább olyan mértékű szakmai kihívás, mint egy hagyományos fegyveres konfliktusé, a szóba jöhető rendkívüli intézkedések köre is ennek megfelelően rendkívül változatos. Mindezen szempontokra figyelemmel, élve az Alaptörvény adta lehetőséggel,[20] az alacsonyabb szintű szabályozás már nem súlyoz a bevezethető intézkedések kapcsán az egyes különleges jogrendi esetkörök között, hanem valamennyi intézkedés meghozatalának lehetőségét biztosítja a szükségesség és arányosság mércéjének[21] érvényesítése mellett.

[19] Alaptörvény 48. cikk (1) Az Országgyűlés…

b) a törvényes rend megdöntésére vagy a hatalom kizárólagos megszerzésére irányuló fegyveres cselekmények, továbbá az élet- és vagyonbiztonságot tömeges méretekben veszélyeztető, fegyveresen vagy felfegyverkezve elkövetett súlyos, erőszakos cselekmények esetén szükségállapotot hirdet ki *(Az Alaptörvény kilencedik módosítását megelőző szövegváltozat).*

[20] „52. cikk (1) Különleges jogrendben az Alaptörvény alkalmazása nem függeszthető fel.

(2) Különleges jogrendben az alapvető jogok gyakorlása – a II. és a III. cikkben, valamint a XXVIII. cikk (2)–(6) bekezdésében megállapított alapvető jogok kivételével – felfüggeszthető vagy az I. cikk (3) bekezdése szerinti mértéken túl korlátozható. (…)

(5) A különleges jogrendben alkalmazandó részletes szabályokat sarkalatos törvény határozza meg.

53. cikk (1) A Kormány különleges jogrendben rendeletet alkothat, amellyel – sarkalatos törvényben meghatározottak szerint – egyes törvények alkalmazását felfüggesztheti, törvényi rendelkezésektől eltérhet, valamint egyéb rendkívüli intézkedéseket hozhat."

[21] Gárdos-Orosz Fruzsina: Az alapjogok korlátozása. In Jakab András – Könczöl Miklós – Menyhárd Attila – Sulyok Gábor (szerk.): *Internetes Jogtudományi Enciklopédia*; 2020. [5, 12, 30] és [40–51].

Az Alaptörvény veszélyhelyzetre vonatkozó szabályozása a szabályozási reform során szintén olyan új megfogalmazást kapott, amely biztosít(hat)ja a kiberműveletek kapcsán is a normál jogrendtől eltérő beavatkozást. Különösen igaz ez az esetkör Alaptörvény tizedik módosításával az alábbiak szerint kialakított szövegére:

„51. cikk (1) A Kormány szomszédos országban fennálló fegyveres konfliktus, háborús helyzet vagy humanitárius katasztrófa, továbbá az élet- és vagyonbiztonságot veszélyeztető súlyos esemény – különösen elemi csapás vagy ipari szerencsétlenség – esetén, valamint ezek következményeinek az elhárítása érdekében veszélyhelyzetet hirdethet ki."

Az Alaptörvény kilencedik módosítása szerinti szöveg[22] rugalmasságát a „szomszédos országban fennálló fegyveres konfliktus, háborús helyzet vagy humanitárius katasztrófa" esetkör beszúrása tovább tágította. Érdemes megfigyelnünk, hogy nem önmagában a beszúrt szövegrész bír nagy jelentőséggel, hiszen ezek nagy valószínűséggel, némi kiterjesztő értelmezéssel tekinthetőek lennének élet- és vagyonbiztonságot veszélyeztető súlyos eseménynek. Sokkal inkább annak van jelentősége, hogy az „ezek következményeinek elhárítása érdekében" fordulat így már valamennyi alaptényállásra kiterjedően értelmezendő,[23] azaz meglehetősen távoli kapcsolatot is mutathat a klasszikus esetköröktől.

Az Alaptörvény szintjén ki kell emelnünk azt is, hogy amíg a korábbi szabályozásban a különleges jogrendet „hirdet ki" szóhasználat szerepelt, az új szövegben már kizárólag feltételes módot alkalmaz a jogalkotó („hirdethet ki"), ezzel is hangsúlyozva, hogy ezek a rendelkezések jogi lehetőségként jelentkeznek, nem pedig kényszerként. Ez biztosítja azt, hogy a kiterjesztett felhatalmazás ne jelentsen minden esetben automatizmust a kihirdetés kapcsán, legyen lehetősége az Országgyűlésnek vagy a Kormánynak mérlegelnie az adott esetben – például egy átfogó kibertámadás esetén –, hogy kívánja-e a kérdést a különleges jogrend adta jogosítványokkal kezelni, vagy a normál jogrend eszközrendszerét veszi igénybe. Ez a kérdés visszavezet az objektív válságfogalomról[24] hosszú ideje folyó szakmai diskurzushoz is, amely szerint a válságok megítélésének minden esetben vannak bizonyos kockázatokat magukban rejtő, szubjektív, adott esetben átpolitizált elemei,[25] amelyeket a helyzet várható következményeinek függvényében értékelnie kell a döntéshozónak és akár

[22] 51. cikk (1) A Kormány az élet- és vagyonbiztonságot veszélyeztető súlyos esemény – különösen elemi csapás vagy ipari szerencsétlenség – esetén, valamint ezek következményeinek az elhárítása érdekében veszélyhelyzetet hirdethet ki.

[23] Azaz például így is: „a szomszédos országban fennálló *fegyveres konfliktus*... következményeinek *elhárítása érdekében* veszélyhelyzet hirdethető ki."

[24] Keszely László: A hibrid konfliktusokkal szembeni átfogó fellépés lehetséges kormányzati modelljei. *Honvédelmi Szemle*, 2020/4. szám, 24–48. o. Lásd különösen a „Válságelméleti alapok" alcím alatti részt.

[25] Tálas Péter: Tatárszentgyörgy után... – A biztonság szubjektív percepciójának veszélyeiről. *Nemzet és Biztonság*, 2009/február, 3–8. o.

két teljesen ténybelileg azonos körülményegyüttesnél is születhet eltérő döntés a különleges jogrend kihirdetéséről vagy annak mellőzéséről.

Az alaptörvényi szabályokra vonatkozó rövid áttekintésünket a fentiekre figyelemmel annyiban összegezhetjük, hogy a különleges jogrendi fogalomrendszer rugalmas és kiterjesztő tényállási elemei megnyitották annak lehetőségét, hogy a jogforrási hierarchia alacsonyabb szintjén fellelhető szabályozók tartalma alkotmányossági aggályok nélkül ki tudjon terjedni a kibertérben jelentkező kihívások kezelésére, adott esetben – a defenzív tevékenységen túl – felhatalmazást jelent az aktív műveletek elvégzésére is, amely mellett a különleges jogrendi intézkedéskatalógus egyidejű kiterjesztése és generalizálása további széles fellépési lehetőséget kínál.

3. A VÉDELMI ÉS BIZTONSÁGI TEVÉKENYSÉGEK ÖSSZEHANGOLÁSÁRÓL SZÓLÓ 2021. ÉVI XCIII. TÖRVÉNY ÉS A KIBERTÉR KIHÍVÁSAI

A védelmi és biztonsági tevékenységek szabályozási reformjának központi eleme a védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvény (Vbö.), amellyel összefüggésben a kibertérből érkező kihívások kapcsán az alábbi szempontokat érdemes felvillantanunk.

A Vbö. keretszabályként jelentkezik, valamennyi a magyar nemzet védelmével és biztonságának fenntartásával és fejlesztésével összefüggő jogszabályi rendelkezéseket erre a törvényre figyelemmel kell meghatározni.[26]

A szabályozás keretjellegéből adódóan, a törvény magában foglalja mindazokat az irányítási, tervezési és szervezeti rendelkezéseket, amelyek a kibertér és a kibertérműveleti képességek kapcsán értelmezhetőek, egyes esetekben ezekre a rendelkezésekre vezethetőek vissza más jogszabályok kapcsolódó szabályai.

A Vbö. olyan kereteket is megfogalmaz, amelyek a korábbi szabályozásban nem vagy csak egyes elemeiben voltak fellelhetőek. A törvény szakmai megközelítésének alapja a lehető legszélesebb körű együttműködés, a „whole of government approach" szemlélet[27] érvényesítése az államszervezetben, és a „whole of society app-

[26] Vbö. 1. § második fordulata.

[27] További adalékok a téma kihívásai és alapvetései kapcsán az összkormányzati megközelítéssel összefüggésben: Tom Christensen – Per Lægreid: The Whole-of-Government Approach to Public Sector Reform. *Stein Rokkan Centre for Social Studies – Working Paper*, 2006/6. szám, 1–29. o.; OECD DAC Guidelines and Reference Series: Whole Of Government Approaches To Fragile States; OECD, 2006 [0020067A1cov.indd (oecd.org)]; illetve kifejezetten a kibervonatkozású kapcsolódásokról: John P. Carlin: Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats. *Harvard Law School National Security Journal*, 2016; 391–436. o., különösen 396, 422. o.

roach"[28] alkalmazása a teljes védelmi és biztonsági terület valamennyi kapcsolódása vonatkozásában.

Maga a tételes szabályozás a Vbö. szintjén egyetlen rendelkezést tartalmaz[29] a kibertér kapcsán, amely azonban több feladatot és felhatalmazást is magában foglal. Ennek értelmében a Kormány a védelmi és biztonsági feladatok összehangolt irányítása keretében nemcsak a katonai és a polgári kibertérműveleti erők védelmi, támadásmegelőzési feladatait, de a nemzetközi műveletekkel, és felkészüléssel összefüggő feladatait is jogosult és köteles meghatározni, amelyhez kapcsolódnak az ezekkel összefüggő kivételes döntéshozatal keretei is.

Mindezeket a szabályokat olyan módon kell a Kormánynak megalkotnia, hogy ezzel összefüggésben az irányítása alá nem tartozó szervekkel való együttműködés is biztosítható legyen. Tanulmányunk összeállítása időpontjában ezek a szabályozók még nem állnak rendelkezésre, de annyi már most látható, hogy ezek sorában egyes elemek nagy valószínűséggel minősített szakmai tartalmú eljárások vagy a nyilvánosság számára nem megismerhető belső szabályozók lesznek, mint ahogy az is valószínűsíthető, hogy a kibertérműveleti erők alkalmazására vonatkozó feladatszabás nem feltétlenül jogszabály formában születik majd meg, adott esetben egyedi döntés is lehet.

A kibertér kihívásainak kezelése, kezelhetősége némi párhuzamot mutathat a terrorista céllal eltérített légi járművek elleni tevékenység (RENEGADE műveleti koncepció[30]) jogi alapjaival és ennek szakmai szempontrendszerével. Egy aktív támadó kiberművelet megítélése jogi szempontból meglehetős hasonlóságot mutat egy 2001. szeptember 11. típusú támadáshoz annyiban, hogy a lefolyása rendkívül gyors, az elkövető beazonosítása előzetesen lényegében lehetetlen, ahogy az is, hogy a támadás felelőssége valamely államhoz legyen kapcsolható, ezzel megalapozva a

[28] Chapter 5 Whole-of-Society; in OECD (2020), OECD Public Integrity Handbook, OECD Publishing, Paris 77–92. o. (https://tinyurl.com/mt5menme); illetve egy szűkebb aspektusban elemzve a „whole of society" kérdését: Mikael Wigell – Harri Mikkola – Tapio Juntunen: *Best Practices in the Whole-of-Society Approach in Countering Hybrid Threats.* European Parliament; Directorate-General for External Policies Policy Department 2021. (Best Practices in the whole-of-society approach in countering hybrid threats (https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU(2021)653632_EN.pdf); Andrew G. McClelland – Roisin Jordan – Szymon Parzniewski – Duncan Shaw – Nat O'Grady – David Powell: Post-COVID Recovery and Renewal through Whole-of-Society Resilience in Cities. *Journal of Safety Science and Resilience*, 2022/3. szám, 222–228. o.

[29] Vbö. 46. § (1) bekezdés j) pont.

[30] Ennek részletei minősített dokumentumokban lelhetőek fel. A nyilvánosan elérhető források közül a NATO, illetve a tagállamok saját doktrinális dokumentumaiban, tájékoztatóiban azonosítható be a feladat. Lásd például: Honvédelmi Minisztérium tájékoztatója 2008, RNG_HM honlapra _2008.01.24_ (honvedelem.hu); NATO Handbook, Brussels 2006; 25. o. [2122 OTAN EN p001-012.ps, page 1-12 @ Normalize (2122 OTAN EN p001-012.indd) (nato.int)]; NATO Encyclopedia 2019; Brussels, 584. o. (2019-nato-encyclopedia-eng.pdf); Doctrine Of The Armed Forces Of The Czech Republic, 2004, Prague, 102. o. [Doctrine of the Armed Forces of the Czech Republic (ethz.ch)].

nemzetközi jogban elfogadott reakciókat. Ugyanakkor az ellentevékenységre és az ezzel összefüggő döntéshozatalra rendelkezésre álló idő rövid, amely időtartam alatt szélsőségesen súlyos károk okozhatóak. Az ellentevékenység jogi alapja pedig hasonló lehet a végszükség, az ENSZ által is elismert önvédelem, illetve a hazai szabályozásban jelenleg váratlan támadásként meghatározott helyzettel – ahogy az a RENEGADE kapcsán is történik.

Figyelemmel egy esetleges kibertámadás jellegére vagy az ennek elhárításához szükséges aktív művelet sajátosságaira, célszerű – adott esetben akár 3000-es kormányhatározati formában – előzetes felhatalmazásokat biztosítani a védekezést végrehajtó, jellemzően nemzetbiztonsági szervezetek számára.

A Kormány kibertérhez kapcsolódó döntései során azt is mérlegelni szükséges, hogy a nyilvánosan hozzáférhető jogforrások nem jelentenek-e tartalmukban önmagukban kockázatot azzal, ha az egyes eljárásokról túlságosan sok árulkodó részletet tartalmaznak. Erre figyelemmel az ilyen felhatalmazó döntéseknek minden esetben csak olyan szintű konkrétumokat célszerű meghatározni, amelyek elégségesek arra, hogy a műveletre vonatkozó döntési felelősség és felhatalmazás egyértelmű legyen a végrehajtó és a jogszerűséget vizsgáló számára, azonban magát a módszert és a pontos technikai eljárást semmi esetre sem tanácsos konkrétan felfedni.

A Vbö. szintjén vizsgálva a kibertérhez kapcsolódó jogosítványokat, ki kell emelnünk azt a tényt, hogy a teljes különleges jogrendi intézkedéskatalógus is a Vbö.-ben kapott helyt, így 2022. november 1-jét követően megszűnik az a fajta részletes és zárt beavatkozásilehetőség-lista, amelyet a korábbi különleges jogrendi szabályozási megközelítés képviselt. Az Alaptörvény kilencedik módosításának hatálybalépését megelőzően a különböző bevezethető rendkívüli intézkedéseket a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény és a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrend idején bevezethető intézkedésekről szóló 2011. évi CXIII. törvény széttagoltan rögzítette, amely felsorolásában egyáltalán nem tartalmazott kifejezetten a kibertérrel összefüggő intézkedési lehetőséget. Az egyetlen olyan rendelkezés, amely némi távoli kapcsolatot mutat tanulmányunk tárgyával, a postai, az elektronikus hírközlési szolgáltatások szüneteltetése, korlátozása és ellenőrzése, továbbá a távközlési és informatikai hálózatok és eszközök, valamint az elektronikus hírközlő berendezések igénybevétele, használatra való átengedése, illetve használatának mellőzése, továbbá a javítókapacitások biztosítása kapcsán jelenik meg.[31]

Ezzel szemben a Vbö. azt a megközelítést választotta, hogy az egyes rendkívüli intézkedések nem jelennek meg tételes felsorolásként, hanem témacsoportokba foglalva, rugalmas listaként szerepelnek.[32] Ez a megoldás gyakorlatilag – a szüksé-

[31] A honvédelemről és a Magyar Honvédségről, valamint a különleges jogrend idején bevezethető intézkedésekről szóló 2011. évi CXIII. törvény 68. § (5) és (5a) bek.

[32] Vbö. 80. § (2) bekezdés.

gesség és az arányosság követelményi keretein belül – korlátlan beavatkozást biztosít a kiberműveleti képességek alkalmazása kapcsán, különös figyelemmel a Vbö. gazdaság- és ellátásbiztonsággal, az állami és önkormányzati működéssel, illetve a törvényes rend, a közrend és a közbiztonság megóvásával vagy helyreállításával összefüggő rendkívüli intézkedésre vonatkozó rendelkezéseire. A mozgásteret tovább bővíti a felsorolást záró utolsó elem, amely a hadiállapotot, a szükségállapotot, a veszélyhelyzetet kiváltó esemény megelőzésével, kezelésével, felszámolásával, továbbá káros hatásainak megelőzésével, illetve elhárításával közvetlenül összefüggő bármely egyéb további területen is lehetőséget biztosít.

A Vbö. azonban nem kizárólagosan a különleges jogrend időszakában alkalmazandó, a béke időszaki összkormányzati válságkezelés során sem kizárt aktív vagy passzív kibertevékenység, amelynek jogalapja nemcsak a Vbö.-ben, hanem például a honvédelemről és a Magyar Honvédségről szóló 2021. évi CXL. törvényben is megjelenik. Az összkormányzati válságkezelés intézménye az összehangolt védelmi tevékenység[33] időszakában teljesedik ki, amely során a Kormány rendeletében meghatározott korlátozásokat és egyéb intézkedéseket vezethet be. A tételes szabályozás bár nem említi a kibertér kihívásainak kezelését, azonban a Vbö.-re általánosan jellemző rugalmas szabályrendszer egyes elemei ezt nem zárják ki. Kiemelendő ezek sorából a Vbö. 76. § azon rendelkezése, amely a kijelölt közterületek és intézmények biztonságának fokozását szolgáló megközelítéskorlátozási, ellenőrzési és védelmi rendszabályok alkalmazását teszi lehetővé. E felsorolás utolsó eleme – hasonlóan a különleges jogrendre vonatkozó felsoroláshoz – biztosítja a listában nem szereplő további, alapjogot nem korlátozó intézkedések bevezetését, azonban ezeknek az intézkedéseknek törvényben kell szerepelniük, és az összehangolt védelmi tevékenységet megalapozó esemény kezelésével, felszámolásával, továbbá káros hatásainak megelőzésével, illetve elhárításával közvetlenül összefüggésben kell lenniük.

A törvény egészét megvizsgálva megállapítható az is, hogy a kibertérrel összefüggő feladatok nem csupán olyan vonatkozásban lehetnek érintettek ebben a szabályozásban, hogy magára a kibertevékenységre vagy az ezzel összefüggő védekezési eljárásokra tartalmaznak rendelkezést. A Vbö. keretjellegéből adódóan a törvény néhány más alapintézményét is érdemes felvillantanunk, ahol szóba kerülhetnek a kibertér kihívásai.

Elsőként a tervdokumentumok rendszerét kell említenünk, amelynek többszintű szabályozása áttételesen kötelezettséget fogalmaz meg a különféle állami szerveknek a védelmi és biztonsági tervezés feladatainak elvégzésére. Ennek keretében nem megkerülhető a kibertevékenységeket érintő tervezési feladatok ellátása sem. A törvény legmagasabb szinten a biztonság és védelempolitikai alapelveket határozza meg tervdokumentumként, amelyet az Országgyűlés bocsát ki.

[33] Vbö. 74. §.

A ma hatályos és a Vbö. hatálybalépését követően felülvizsgálandó 94/1998. (XII. 29.) OGY határozat idevonatkozóan azt fogalmazza meg, hogy „fokozódó kihívást és veszélyt jelent… az információs rendszerek elleni támadások lehetősége".

Megjelenik a kérdés a Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1163/2020. (IV. 21.) Korm. határozatban is, amely szintén alapvető – és az Alaptörvény kilencedik módosítását követően újraalkotandó – biztonsági tervdokumentum. A Nemzeti Biztonsági Stratégia már jóval szofisztikáltabban és nagyobb részletezettséggel jeleníti meg a kibertér kihívásait, kezdve a hibrid támadások elleni ellenálló képesség eszközeként történő megnevezésétől, az elektronikus információs rendszerek sérülékenységén át, a kiberteret kritikus adatok illegális megszerzésére, valamint az elektronikus információs rendszerekben vagy azokon keresztül történő – akár fizikai – károkozásra történő felhasználásán keresztül, a kibertérben jelentkező kihívások, kockázatok és fenyegetések kezelésére, a megfelelő szintű kiberbiztonság garantálására, a kibervédelmi feladatok ellátására, a nemzeti létfontosságú információs infrastruktúra zavartalan működésének biztosításáig.[34]

A stratégia arra is rámutat, hogy az új biztonsági kihívások miatt folyamatosan szükséges fejleszteni az információs és kiberhadviselés elleni védekezés rendszerét.

A Vbö. tervdokumentum-struktúrájában harmadikként szereplő integrált védelmi és biztonsági iránymutatás nem rendelkezik a fentiekhez hasonló szabályozási előzményekkel, azonban ennek előírt tartalma[35] és funkciója kifejezetten azt vetíti előre, hogy a kiberkihívások kezelése kiemelt hangsúlyt fog kapni. Ez a dokumentum nagy valószínűséggel minősített elemeket is tartalmazni fog, így a jogalkotó alacsonyabb kockázattal lesz képes tervezni az ilyen irányú működési eljárásokat és fejlesztéseket.

A tervezés negyedik szintje az ágazati törvényekben vagy a Kormány rendeletében előírt ágazati, illetve kihívás- vagy fenyegetésközpontú, továbbá kockázatelemzésen alapuló stratégiák, alaptervek, illetve intézkedési tervek csoportja. Ezen a szinten már nem egy-egy tervdokumentumról beszélünk, így a kibertérrel összefüggő feladatok több párhuzamos tervben is megjelennek majd, mint például a

[34] Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1163/2020. (IV. 21.) Korm. határozat 31., 71. és 152. pontok.

[35] Vbö. 22. § (5) Az Integrált Védelmi és Biztonsági Iránymutatás a Biztonság- és Védelempolitika Alapelveire, valamint a Nemzeti Biztonsági Stratégia alapján – a nemzetbiztonsági érdekek és minősített adatok védelmének elsőbbségére figyelemmel – a Kormány határozatában kiadott tervezési dokumentum, amely hosszú távra határozza meg

a) az ország védelmi és biztonsági érdekeinek érvényesítéséhez szükséges képességcélokat,

b) az ország biztonságának fenntartásához és megerősítéséhez szükséges részletes cselekvései irányokat,

c) az ország védelmével és biztonságával összefüggő átfogó feladatrendszerben érintett szervek együttműködésének főbb irányait, valamint

d) az a)–c) ponttal összefüggő főbb ágazati feladatokat.

létfontosságú rendszerelemekre vonatkozó tervek, az egyes szervezetek honvédelmi intézkedési tervei, a kifejezetten kiberbiztonságot célzó dokumentumok.

Itt emelném ki a tervezés mint intézmény jelentőségét, amely nem csupán papírgyártást jelent, hanem a költséghatékony és összehangolt fellépés záloga is egyben. A tervezés során vagyunk képesek beazonosítani, hogy milyen kockázatokat és milyen eszközökkel kell/lehet kezelnünk, mire és milyen eljárásban vagyunk képesek, és milyen fejlesztésekre van szükségünk. A tervezés az alapja a felkészítésnek és a védekezés/támadás egyes feladatai begyakorlásának is.

A fentieken túl a Vbö. szabályrendszere önálló fejezetet szentel a nemzeti ellenálló képességnek is. Ez a fejezet leképezi a NATO resilience megközelítés[36] fő irányait, lényegében azonos tartalommal – egy kiegészítéssel (felkészültség, elhivatottság) – jeleníti meg az ismert követelményrendszer hét elemét.[37] A felsorolás szerinti területeken az ellenálló képesség megvalósítása kivétel nélkül magas fokú kiberbiztonságot követel meg, legyen szó akár az államszervezet, a kormányzás folyamatos működéséről, akár az energetikai vagy közlekedési infrastruktúra ellenálló képességéről, de még a sérültek tömeges ellátási képességének biztosítása sem nélkülözheti az alapvető kiberbiztonsági szempontok érvényesítését. Mindez azt is jelenti, hogy ahogyan a NATO és hazánk is lényeges szempontrendszerként kezeli ezeket a területeket, úgy az esetleges támadó szándékkal fellépni szándékozó szereplők számára is ezek azok az elsődleges célpontok, amelyekben kárt kell okozniuk, ha gyengíteni akarják védelmi képességeinket. Első ránézésre a hét resilience alapkövetelmény nem érinti a klasszikus katonai képességek védelmét, ez azonban csak látszólagosan van így, hiszen a kormányzás és az államszervezet működésének folytonossága feltételezi a katonai szervezetek működési folytonosságának kvázi-zavartalanságát is.

A Vbö. kapcsán a kibertér irányából érkező fenyegetésekhez kapcsolódóan nem mehetünk el a gazdasági és anyagi szolgáltatási kötelezettség intézménye mellett sem. Ennek az a célja, hogy amennyiben az ország védelmével és biztonságával közvetlenül összefüggő, törvényben meghatározott feladatok ellátásához nem állnak rendelkezésre a megfelelő anyagi és szolgáltatási feltételek, lehetőség legyen annak biztosítására nem állami erőforrások felhasználásával.

A jelenlegi rendszerben ennek pontos szabályait végrehajtási rendeletek[38] tartalmazzák, amelyekkel összefüggésben szembetűnő, hogy elsősorban járművek, munkagépek jelennek meg, nincs kimondott lehetőség informatikai eszközök biztosítására. Évtizedekkel ezelőtt ennek a kérdésnek még korántsem volt akkora jelentősége, mint manapság. Egy megfelelően célzott kibertámadással az állam valamennyi

[36] Wolf-Diether Roepke – Hasit Thankey: Resilience The First Line Of Defence. *The Three Swords Magazine*, 2019/34. szám, 50–53. o.

[37] Vbö. 42. §.

[38] A honvédelemről és a Magyar Honvédségről, valamint a különleges jogrend idején bevezethető intézkedésekről szóló 2011. évi CXIII. törvény végrehajtásáról szóló 290/2011. (XII. 22.) Korm. rendelet.

alapvető védelmi funkciója bénítható, vagy akár fizikailag is megsemmisíthetőek meghatározó informatikai eszközök, így amennyiben ezen a területen nem áll rendelkezésre megfelelő állami tartalék, a kieső kapacitások pótlása csak a nemzetgazdaságból lesz lehetséges. A Vbö. hozta újítás is – ti. a gazdasági és anyagi szolgáltatási kötelezettség valamennyi szabályát egységesen tartalmazza függetlenül attól, hogy katasztrófavédelmi vagy honvédelmi célú felhasználásról van szó – lehetőséget ad arra, hogy a végrehajtási rendelet szintjén ez a lista megfelelően kiegészüljön, és a védekezés valamennyi szegmensére kiterjeszthető legyen.

A NATO Válságreagálási Rendszerével összhangban álló Nemzeti Intézkedési Rendszer alkalmazásának és az EU-válságkezelésben való nemzeti részvétel alapvető szabályainak Vbö.-ben szabályozott rendszere szintén jelentős összefüggést mutat a kiberműveletekkel. A NATO Crisis Response Systemben alkalmazott intézkedéskatalógus egy olyan, számos elemében minősített lista, amelyek alkalmazásának elrendelésével konkrét kiber(ellen)tevékenységekre vagy az ezekre történő közvetlen felkészülésre is sor kerülhet. A Nemzeti Intézkedési Rendszer jelenleg lényegében a NATO rendszerének hazai adaptálása, azonban a Vbö. a végrehajtási rendeleti szinten megfogalmazott célkitűzése a hazai intézkedési rendszer határainak kiterjesztése azon területekre, amelyek nem a klasszikus fegyveres fenyegetésekhez kapcsolódóan is szóba jöhetnek, legyen az élelmiszer-ellátási válság, egészségügyi válság vagy más olyan működési zavar, amelynek biztonsági következményei lehetnek. Ezek mindegyike – ahogy azt fentebb a rezilienciánál jeleztük – összekapcsolható lesz a kibertérben folytatott tevékenységekkel.

4. A HONVÉDELEMRŐL ÉS A MAGYAR HONVÉDSÉGRŐL SZÓLÓ 2021. ÉVI CXL. TÖRVÉNY ÉS A KIBERTÉR KIHÍVÁSAI

Tekintettel arra, hogy a Vbö. keretszabály, az egyes ágazatokhoz köthető további törvények lényegesen részletesebb tartalommal foglalkozhatnak a kiberműveletekkel. A Vbö. megalkotása az egyes feladatok integrálására és szabályozási tárgyak egységesítésére, valamint a cím módosításának elkerülhetetlenségére figyelemmel szükségessé tette a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrend idején bevezethető intézkedésekről szóló 2011. évi CXIII. törvény teljes újraszabályozását, amelynek eredményeként 2022. november 1-jén hatályba lép a honvédelemről és a Magyar Honvédségről szóló 2021. évi CXL. törvény (Hvt.).

A Hvt. – a NATO általános megközelítésével összhangban – a kiberteret műveleti területként definiálja. A Magyar Honvédség katonai kibertérműveleti erői folyamatosan ellátják a honvédelmi szervezetek kibertérből érkező fenyegetésekkel és támadásokkal szembeni védelmét, végrehajtják a kibertérből érkező támadás megszakításához szükséges intézkedéseket, illetve a Magyarország biztonságát, illetve szövetségesi kötelezettségeit sértő vagy fenyegető rendszerekkel szembeni katonai

kibertérműveleti fellépést.[39] Az aktív (védekezési céllal támadó) kiberműveletre megfelelő szintű közjogi döntés birtokában (ez a beavatkozás jellegének függvényében akár Kormány vagy Országgyűlés is lehet), kizárólag szövetségi kötelezettség teljesítésének keretében, nemzetközi művelettel összefüggésben vagy honvédelmi válsághelyzetben van lehetőség a kibervédelmi ügyeletes parancsnok döntése alapján.

A Hvt. vonatkozó szakasza szerint különleges jogrendben kizárólag a Kormány hozhat ilyen döntést, amely azonban meglehetősen furcsa rendelkezés, hiszen a különleges jogrend esetei eltérő jellegűek, nem összehasonlítható egy veszélyhelyzeti döntés súlya és hatása a hadiállapotban hozott döntésekkel még akkor sem, ha maga a döntés szakmai tartalom oldaláról teljes mértékben megegyezik.

A törvény speciális kárfelelősségi szabályozást is rendel a kiberműveletekhez,[40] amelyek garantálják a művelettel okozott sérelem minimalizálását, a közvetlen fenyegetéssel arányos, ugyanakkor határozott fellépést.

A Vbö. keret- és a Hvt. szubszidiárius, komplementer viszonyát a honvédelmi válsághelyzeti szabályozáson keresztül érhetjük tetten a leglátványosabban. Ezek szerint[41] honvédelmi válsághelyzetben a Vbö.-ben meghatározottak szerint – a Vbö.-ben meghatározott intézkedéseken túl – a Kormány további intézkedéseket vezethet be, amely többek között a KNBSZ és a Honvédség felderítő, elhárító, valamint kibertérműveleti erői tevékenységének fokozását is magában foglalja a fenyegetettség Magyarországra történő átterjedésének, illetve magyarországi felerősödésének megakadályozása érdekében.

5. A KOORDINÁCIÓ JELENTŐSÉGE

A kibertér kihívásainak kezelését a fentieken túl azonban nem kizárólag törvények rendelkezései célozzák, számos rendeleti, kormányhatározati vagy ennél alacsonyabb szintű szabályozó is foglalkozik a kérdéssel. A terület jellegzetessége, hogy hatásai komplexen jelentkeznek, így ez az a szakmai irány, amely egészen biztosan nem választható szét egy-egy ágazatra, a felmerülő kihívásokat szinte kivétel nélkül összkormányzati megközelítést feltételezve lehet eredményesen kezelni. Ilyen módon a kibertérrel összefüggő gyakorlatban is tapasztalt összetett fenyegetések a védelmi és biztonsági reform megalapozásához is jó kiindulópontot jelentettek, az így jelentkező feladatok ágazatokon átívelő hatásain keresztül kiválóan be lehetett

[39] A Hvt. 88. § értelmében ez a tevékenység nem terjed ki a Katonai Nemzetbiztonsági Szolgálat szervezetére.

[40] Hvt. 89. §.

[41] Hvt. 107. §.

mutatni annak szükségszerűségét és indokoltságát, hogy miért is kell a védelem kérdéseit a legmagasabb szinten összehangolni.

Már a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről szóló 484/2013. (XII. 17.) Korm. rendelet közel tíz évvel ezelőtti megalkotása is arra mutat rá, hogy az együttműködés és a folyamatok koordinációja elengedhetetlen ezen a területen.[42]

A védelmi és biztonsági szabályozási rendszer átfogó reformja hosszabb távon olyan eredményt is hozhat, hogy valamennyi védelmi és biztonsági terület összkormányzati szintű koordinációja egy szervezet égisze alatt valósul meg. Ez nem azt jelenti, hogy a különféle munkacsoportok, tárcaközi bizottságok működése feleslegessé válik, és minden központosítottan zajlik. Sőt, kifejezetten hasznos a szakmai mélységeket sem nélkülöző ágazatközi együttműködés, mindezt azonban a más védelmi és biztonsági szakterületek kapcsolódásaira is figyelemmel célszerű megvalósítani, ebben segíthet a központi koordinációs szerepkör. A jelenlegi szabályozási környezet – és ez részben igaz a kibertevékenységgel összefüggő szakterületekre is – azokat a megoldásokat preferálja, amelyek inkább az egyes miniszterek felelősségéhez kötik a tevékenységeket, miközben jó néhány olyan kihívást tudunk megnevezni, amelyek kezelése egészen biztosan nem állhat meg miniszteri szinten. Jó példa volt erre a Covid pandémia kezelése, amely során az egészségügyért felelős miniszter tevékenysége a válságkezelésben már-már sokadlagosnak nevezhető a nemzetgazdaság, a jogalkotási folyamatok vagy az oktatási rendszer működésének fenntartása, illetve az államszervezet, a központi és területi igazgatás általános működésének biztosításához kapcsolódó feladatok tükrében.

***

A fenti szabályok mind az alaptörvényi, mind a sarkalatos törvényi szinten történő megjelenése egy olyan szakmai folyamat jogszabályban is jól látható első jelének tekinthető, amely meggyőződésem szerint messze nem áll meg ezen a szinten. A kiberfenyegetések kiterjedtsége és eszköztárának bővülése, a támadások mindennapossá válása,[43] a hibrid hadviseléssel való összekapcsolódásai egyaránt azt prognosztizálják, hogy az ilyen jellegű szabályok számossága növekedni fog. Nem egészen két évtizedet visszalépve az időben ez a fajta kihívásintenzitás elképzelhetetlen

[42] A rendelet megalkotásának törvényi alapja a 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

[43] A Live Cyber Threat Map | Check Point weblap adatai szerint 2022. október 1-én 0:00 és 22:08 perc között 34 728 056 kibertámadás történt. Az elmúlt év napjainak statisztikáit áttekintve ez nem számít kiemelkedőnek, hiszen olyan nap is volt, amikor az észlelt kibertámadások száma elérte a 120 000 000-t. Egy másik adatbázis szerint (Live Threat Map | Real-time View of Cyber Attacks | Imperva) 859 414 284 támadási kísérlet történt 2022. szeptember 30-án, amelyből 78 779-et Magyarországról indítottak, miközben az országot 135 389 támadás érte.

volt, a 2004. évi CV. törvény a honvédelemről és a Magyar Honvédségről még egyáltalán nem szabályozott ebben a tárgykörben.

Összességében értékelve a fentieket, láthatjuk, hogy az alaptörvényi szabályokon túl a sarkalatos törvényeken át, a végrehajtási szabályozókig bezárólag a védelmi és biztonsági tevékenységre vonatkozó szabályozási reform egyik alapvető mozgatórugója éppen az a felismerés volt, hogy a 21. századi technológiai fejlődés és az ebből következő új biztonsági kihívások, valamint a hagyományos biztonsági kihívások súlypontjainak áthelyeződése megoldandó feladatként jelentkezett a hazai védelmi és biztonsági szabályozásban, melyek elmaradása több területen – a kibertevékenységekkel összefüggésben pedig kifejezetten hangsúlyosan – biztonsági deficitet eredményezett volna, szélsőséges esetben maga az elavult szabályozás képezte volna akadályát az egyébként technikailag lehetséges védelmi célú passzív és aktív tevékenységek végrehajtásának.

BÁNYÁSZ PÉTER – KRASZNAY CSABA – TÓTH ANDRÁS

A kibervédelem szakpolitikai szintjének helyzete és kihívásai Magyarországon, az EU-ban és a NATO-ban

2022 végén úgy véljük, magabiztosan kijelenthető, a kiberbiztonság életünk minden szegmensében létfontosságú. A bennünket körülvevő infokommunikációs eszközök nem csupán a társadalmi együttélés, hanem a társadalmi-politikai közeg működését biztosító infrastruktúrák megkerülhetetlen részévé váltak. A technológiai fejlődés, a mindent behálózó internetes eszközök azonban roppant törékeny ökoszisztémát alakítottak ki, amelynek akár kismértékű sérülése is komplett rendszereket tehet tönkre.

2007-ben Észtország kormányzati és gazdasági létfontosságú rendszerelemeinek hetekig tartó kibertámadása felkészületlenül érte a megtámadott országot, illetve szövetségeseit. Észtországot NATO-tagállamként érte ez a támadás, azonban senki nem tudott választ adni, hogy milyen lépéseket adhatna a NATO mint katonai védelmi szövetség. A bizonytalansággal a NATO nem volt egyedül, számos ország próbálta értelmezni azt az új stratégiai helyzetet, ami az észt rendszereket érte a kibertérből. Mindez elindított egy rendkívül intenzív stratégiai és szabályozási gondolkodást, ami nem csupán a kibervédelmi ellenálló képességre, de a reagálóképesség kialakítására is vonatkozott.

2007 óta sok bit lefolyt az optikai kábelekben, számos olyan paradigmaváltó esemény következett be (például a 2016-os amerikai elnökválasztásba történő beavatkozás, az új típusú koronavírus-járvány kiberbiztonsági aspektusai, a 2022 februárja óta zajló ukrán–orosz háború), amelyek a megalkotott stratégiák újragondolását követelték meg a biztonsági közeg változási kényszere miatt.

A tanulmány ezt a stratégiai fejlődést kívánja feldolgozni a címben szereplő három entitás aspektusából. Mivel a kiberbiztonság egy rendkívül komplex szakterület, így a kiadvány terjedelmi korlátai nem teszik lehetővé, hogy az egyes stratégiai dokumentumokat a szerzők részletesen vizsgálják. Remélhetőleg e közlemény eligazodást nyújt a stratégiai dokumentumok sűrűjében.

1. A KIBERVÉDELEM SZAKPOLITIKAI SZINTJÉNEK HELYZETE ÉS KIHÍVÁSAI MAGYARORSZÁGON

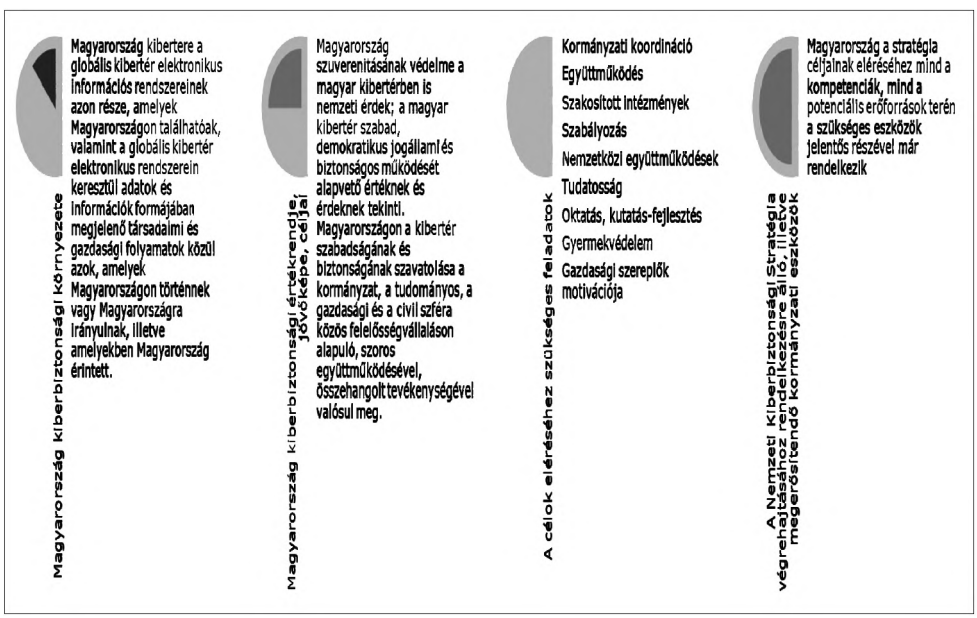
Magyarországon az elektronikus információbiztonság szabályozása hosszú múltra tekint vissza. Az első vonatkozó rendelkezés 1981-ben jelent meg, amikor az 1/1981. (I. 27.) BM rendelet a számítástechnikai rendszerek titok-, vagyon- és tűzvédelméről hozta be a közgondolkodásba az elektronikus információs rendszerek védelmét. Ezt követte 1987-ben a 3/1988. (XI. 22.) KSH rendelkezés az államtitok és szolgálati titok számítástechnikai védelméről. Ezek a jogszabályok is mutatják, hogy a magyar szabályozás már a rendszerváltás előtt is komolyan vette a frissen megjelenő informatikai rendszerek információbiztonsági szempontú védelmét, melyet a rendszerváltást követően, az informatika széles körű közszolgálati elterjedésével párhuzamosan számos más szabályozás is követett.

1994-ben a Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága jelentette meg az Informatikai Biztonsági Módszertani Kézikönyvet, melyet MEH ITB 8-as számú ajánlásként ismerünk. Ezt követte 1996-ban, szintén a Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottságának kiadásában az Informatikai Rendszerek Biztonsági Követelményei, azaz a MEH ITB 12-es számú ajánlás, mely sorozatot 1997-ben a Common Criteria szabvány magyar fordítása, az Informatikai termékek és rendszerek biztonsági értékelésének módszertana, azaz az ITB 16-os számú ajánlás zárt le. Az 1990-es években tehát megteremtődött annak a lehetősége, hogy a magyar közszolgálat az akkor legfrissebb szabványokból, a ma ISO 27000-ként és ISO 15408-ként ismert szabványokból tudjon magyar nyelven dolgozni.

Az 1990-es évek ajánlásai hosszú ideig érvényben voltak, egészen a 2000-es évek második feléig, 2008-ig nem jelent meg olyan új kiadvány, amely lehetővé tette volna azt, hogy a magyar közszolgálat elektronikus információbiztonsága lépést tudjon tartani a rohamosan változó technológia jelentette új típusú fenyegetésekkel. 2008-ban a Miniszterelnöki Hivatal Közigazgatási Informatikai Bizottsága adta ki a Magyar Informatikai Biztonsági Ajánlások (MIBA), azaz a KIB 25. számú ajánlásnak új köteteit, melyben egyrészt az ISO 27000 szabványhoz hasonló, másrészt pedig az ISO 15408 (Common Criteria) szabványt feldolgozó ajánlások jöttek létre Magyar Informatikai Biztonsági Keretrendszer (MIBIK), illetve Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS) néven. Ezt egészítette ki az az ajánlás, mely a kis szervezetek számára nyújtott útmutatót az információbiztonság megvalósítása érdekében (Informatikai Biztonsági Iránymutató Kis Szervezetek Számára – IBIX). A 2000-es években jött létre az az intézményrendszer, mely lehetővé tette a magyar közszolgálat komplex védelmét a kibertérből érkező fenyegetésekkel szemben. Ekkor a Puskás Tivadar Közalapítvány (PTA) keretében működő CERT-Hungary Központ lett a magyar kormány hálózatbiztonsági központja. A közigazgatási hálózatbiztonsági központ felállítása céljából a PTA az Informatikai

és Hírközlési Minisztérium támogatásával 2004-ben kezdte meg a CERT-Hungary program beindítását.[1]

Az igazán jelentős változások a magyar információbiztonság szabályozásában viszont a 2010-es évektől kezdődtek el. Ennek az első jele a 1035/2012. (II. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról volt. Ebben a jogszabályban a kiberteret már mint komoly fenyegető tényezőt jelölik meg a jogalkotók, felhívva a figyelmet arra, hogy szükségessé vált egy olyan komplex szabályozási rendszer létrehozása, melynek segítségével Magyarország felkészülhet az internetről, tágabb értelemben pedig a kibertérből érkező fenyegetések kezelésére. A 2012-es Nemzeti Biztonsági Stratégiából eredeztethetően jelent meg a 1139/2013. (III. 21.) Korm. Határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról, mely az első olyan jogszabály volt a magyar jogrendben, mely kimondottan a kibertér biztonságával foglalkozott. A 2013-as kormányhatározat jelenleg is érvényben van, így annak frissítése elkerülhetetlen. A 1163/2020. (IV. 21.) Korm. Határozat Magyarország Nemzeti Biztonsági Stratégiájáról egyértelműen leírja, hogy a 2013-as Nemzeti Kiberbiztonsági Stratégia elavult, és számos olyan változás történt a fenyegetési térben, mely indokolja egy új stratégia kibocsátását. Eszerint:


Magyarország kiberbiztonsági környezete
Magyarország kibertere a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve amelyekben Magyarország érintett.
Magyarország kiberbiztonsági értékrendje, jövőképe, céljai
Magyarország szuverenitásának védelme a magyar kibertérben is nemzeti érdek; a magyar kibertér szabad, demokratikus jogállami és biztonságos működését alapvető értéknek és érdeknek tekinti. Magyarországon a kibertér szabadságának és biztonságának szavatolása a kormányzat, a tudományos, a gazdasági és a civil szféra közös felelősségvállaláson alapuló, szoros együttműködésével, összehangolt tevékenységével valósul meg.
A célok eléréséhez szükséges feladatok
Kormányzati koordináció
Együttműködés
Szakosított intézmények
Szabályozás
Nemzetközi együttműködések
Tudatosság
Oktatás, kutatás-fejlesztés
Gyermekvédelem
Gazdasági szereplők motivációja
A Nemzeti Kiberbiztonsági Stratégia végrehajtásához rendelkezésre álló, illetve megerősítendő kormányzati eszközök
Magyarország a stratégia céljainak eléréséhez mind a kompetenciák, mind a potenciális erőforrások terén a szükséges eszközök jelentős részével már rendelkezik

1. ábra. *1139/2013. (III. 21.) Korm. Határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról.* Forrás: saját szerkesztés

[1] Muha Lajos – Krasznay Csaba: *Az elektronikus információs rendszerek biztonságának menedzselése.* Budapest, Nemzeti Közszolgálati Egyetem, 2018.

„178. A biztonság egyes részterületeiért felelős állami szervezeteknek a Magyarország Nemzeti Biztonsági Stratégiában megfogalmazott iránymutatásokkal összhangban kell megalkotniuk és felülvizsgálniuk a tevékenységükre vonatkozó szakági szabályzókat, különös tekintettel a nemzeti katonai, a rendészeti, a nemzetbiztonsági, a terrorelhárítási, a katasztrófavédelmi, a kiberbiztonsági és a migrációs területekre."[2]

Hozzá kell tenni, hogy 2018-ban az Európai Unió hálózati és információs rendszerek biztonságára vonatkozó (NIS) direktívájának következményeképpen létrejött egy olyan stratégia, mely részben kiegészíti, részben pedig felülírja a 2013-as eredeti stratégiát. Ez a 1838/2018. (XII. 28.) Korm. Határozat Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról, mely szintén érvényben van, így a tanulmány írásának idején két olyan hatályos stratégiával rendelkezik Magyarország, mely a kibertérre vonatkozik, és részben kiegészítik, részben ellentmondanak egymásnak. Az új stratégia megjelenéséig tehát Magyarország érvényben levő Nemzeti Biztonsági Stratégiája jelent útmutatót számunkra azzal kapcsolatban, hogy a magyar kormány miként gondolkodik a kibertér veszélyeiről.


A digitális környezet iránti bizalom erősítése
Szakmai együttműködés erősítése
Biztonságtudatosság növelése
Bűnüldözés - kiberbűnüldözés fejlesztése
A szakmai irányító intézményrendszer fejlesztése
Digitális infrastruktúra védelem
Informatikai fejlesztések minőségmenedzsmentje
Kormányzati elektronikus szolgáltatások biztonságának növelése
Nemzetközi együttműködés erősítése
Alapvető szolgáltatások, valamint a létfontosságú infrastruktúrák és szolgáltatásaik védelme
Kibervédekező, elhárító és reagáló képességek fejlesztése
A gazdasági szereplők támogatása
Kutatóközpontokkal való együttműködés, valamint a kutatás és fejlesztés szerepének erősítése
Hazai digitális innováció támogatása, támogatási konstrukciók kialakítása, koordinációs feladatok ellátása
Versenyképes hazai tudásbázis létrehozása

2. ábra. *1838/2018. (XII. 28.) Korm. Határozat Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról.* Forrás: saját szerkesztés

[2] 1163/2020. (IV. 21.) Korm. Határozat Magyarország Nemzeti Biztonsági Stratégiájáról.

Magyarország Nemzeti Biztonsági Stratégiájának alapvetése a következő:

„Nemzeti szuverenitásunk olyan megkérdőjelezhetetlen alapérték, amely természetes módon van jelen hazánk kül- és belpolitikájában egyaránt. Elsődleges biztonságpolitikai érdekünk a folyamatosan változó viszonyok között a magyar állam önrendelkezésének, cselekvési szabadságának oltalmazása, megőrzése és erősítése. Magyarország és a magyar állampolgárok mindenoldalú – politikai, gazdasági, pénzügyi, társadalmi, technológiai, környezeti, egészségügyi, katonai, rendészeti, információs és kibertérbeli – biztonsága alapvető érték. Biztonságunk megteremtése, fenntartása és erősítése olyan követelmény, amely minden további kormányzati célkitűzés teljesülésének előfeltétele."

Ahogy ebből a tézisből is kiolvasható, a katonai biztonság, illetve az információ- és kibertérbeli biztonság megteremtése egyenlő súllyal jelenik meg a magyar kormány biztonsági gondolkodásában. A Nemzeti Biztonsági Stratégia ezt az alapvetést a továbbiakban részletesen is kibontja. Egyrészt alapvető adottságaink között felsorolja a hibrid támadásokkal szembeni felkészülés igényét, másrészt a kiberbiztonsággal kapcsolatos képességek megteremtésének fontosságát:

„31. Hibrid támadással szembeni ellenálló képességünket növeli a nemzet egysége, demokráciánk szilárdsága, a közös nyelv, a felgyorsított döntéshozatali képesség, valamint a honvédelmi és rendvédelmi erők szoros együttműködése egymással és a releváns polgári infrastruktúrával. Az új biztonsági kihívások miatt azonban folyamatosan szükséges fejleszteni az információs és kiberhadviselés elleni védekezés rendszerét.

32. Magyarország Kormánya mindent megtesz hazánk kiberbiztonsága érdekében, kapacitásainkat e területen is folyamatosan fejlesztjük. Tekintettel arra, hogy a kormányzati és más kulcsfontosságú infokommunikációs rendszerek elleni támadások száma növekszik és kifinomultságuk erősödik, folyamatos erőfeszítés szükséges az infokommunikációs rendszerek védelmének erősítése érdekében. Általános jelenség továbbá a felhasználók információbiztonsági tudatosságának alacsony szintje, holott a felhasználók megfelelő információbiztonsági tudatossága a kiberincidensek megelőzésének egyik kulcseleme."

A Nemzeti Biztonsági Stratégiában tehát megjelenik a belbiztonság, illetve a honvédelem konvergenciája a kibertér védelmének érdekében. Ez nem újdonság, hiszen a magyar kibervédelmi szabályozásban a kezdetektől érzékelni lehet a két védelmi terület egyértelmű lehatárolását, közben együttműködésre késztetését, az évtizednyi jogfejlődésben viszont észrevehetően nőtt a katonai terület fontosságának hangsúlyozása. A nemzetközi példákban egyébként két kiberbiztonsági stratégiaalkotási megközelítéssel lehet találkozni. Az egyik az államközpontú, a másik pedig a külső felek bevonását és együttműködését támogató stratégiaalkotás. Míg az államközpontú stratégiák kimondottan belbiztonsági, illetve katonai feladatként tekintenek a kibervédelemre, és elsősorban az állam, a kritikus infrastruktúrák és a honvédség saját rendszereinek védelmére törekednek, addig más, nyitottabb kiberbiztonsági stratégiák figyelembe veszik az államon kívüli szereplők, így a magánszektorban

működő cégek, az akadémiai szereplők, illetve a civil szervezetek igényeit is, valamint a védelmi megközelítés mellett gazdasági lehetőségként is tekintenek a kiberbiztonságra.[3] Magyarország a stratégiákból jól kiolvasható módon elsősorban belbiztonsági és katonai biztonsági feladatként fogja fel a kibervédelmet, nem törekszik a széles körű bevonásra.

Eközben, amikor Magyarország biztonsági környezetéről ír a Nemzeti Biztonsági Stratégia, számos olyan szempontot is felsorol, mely óhatatlanul igényli az államon és a kritikus infrastruktúraüzemeltetőkön kívül más szereplők bevonását is. A stratégia 48. pontja így fogalmaz:

„A hatalmi vetélkedés mindinkább kiterjed a globális közjavakra is: fokozódó küzdelem folyik a nemzetközi vizek és az ott található erőforrások, az északi sarkvidék és a világűr ellenőrzéséért, valamint a kibertér dominanciájáért. Az emberiség technológiai szintjének rohamos fejlődésével [digitalizáció, ötödik generációs vezeték nélküli hálózat (5G), űrtechnológia, stb.] folyamatosan új lehetőségek és kihívások jelennek meg, amelyek hatást gyakorolnak hazánk biztonságára. Az 5G jelentette technológia olyan forradalmi fejlesztéseket tehet lehetővé perspektivikusan, amelyek számottevő változásokat generálhatnak társadalmunk és gazdaságunk viszonylatában."

Az itt megjelenített technológiák olyan komplex ökoszisztémát jelentenek, melyeket a kritikus infrastruktúrákat szabályozó kiberbiztonsági jogszabályok nem tudnak teljesen lefedni. Az ellátási láncok kiberfenyegetései beláthatatlan hatással vannak a digitális társadalmak és digitális gazdaságok működésére, így azok komplex védelme a szabályozáson túlmenően az állami és nem állami szereplők együttműködésével valósítható meg sikeresen. A nem állami szereplők szerepét pedig nemcsak az együttműködésben, hanem a fenyegetések között is tetten lehet érni.

„69. A technikai fejlődéssel és vívmányainak elterjedésével folytatódik a biztonságot veszélyeztető, nehezen kontrollálható nem állami szereplők – például szervezett bűnözői körök, nemzetközi terrorszervezetek, kiberbűnözői csoportok, szélsőséges vallási közösségek, magán biztonsági cégek, egyes nem kormányzati szervezetek és egyéb transznacionális hálózatok – súlyának növekedése a nemzetközi biztonságpolitikában. Ezek mögött sokszor nehezen azonosítható érdekek és csoportok húzódnak meg, és könnyen szolgálhatnak rejtett állami szándékokat. Mindez átrendezi és áttekinthetetlenebbé teszi egyes térségek biztonsági helyzetét, ami hazánk számára is kihívást jelent.

70. Az információs technológia rohamos fejlődéséből és terjedéséből kifolyólag az állam és a társadalom működése egyre inkább a digitalizációra épül. Az elektronikus információs rendszerek sérülékenységei ezért biztonsági kockázatot hordoznak magukban. Világméretű tendencia, hogy a kibertérben végzett, ártó szándékú tevékenységek egyre gyakoribbak, egyre kifinomultabbak és egyre nagyobb kárral járnak.

[3] Kovács László: *Kiberbiztonság és -stratégia.* Budapest, Dialóg Campus, 2018.

71. Növekvőben van azoknak az államoknak és nem állami szereplőknek a száma, amelyek a kiberteret kritikus adatok illegális megszerzésére, valamint az elektronikus információs rendszerekben vagy azokon keresztül történő – akár fizikai – károkozásra használják. Ezért a kibertér ma már a szárazföld, a tengerek, a levegő és a világűr mellett külön műveleti térnek számít. A jövőbeli konfliktusok nagy valószínűséggel még inkább ki fognak terjedni a kibertérre."

Összegezve, a biztonsági környezet leírásában megjelenik mindaz, ami indukálja a kibervédelem megerősítésének igényét Magyarországon. Foglalkozik az új technológiák megjelenésével, a kiberbűnözés, a kiberhadviselés, a kiberkémkedés, illetve a hacktivista és kiberterrorista csoportok kérdéskörével. Megemlíti az információs műveletek veszélyét is az állami és nem állami szereplők szempontjából, illetve foglalkozik a katonai képességfejlesztés kérdésével is. Ennek során hivatkozik arra, hogy az ötödik műveleti tér, a kibertér is hasonlóan fontos, mint a másik négy műveleti tér Magyarország számára.

Tovább elemezve a Nemzeti Biztonsági Stratégiát, az alapvető érdekeinket felsoroló témák között két érdekes pontot lehet felfedezni. A 101. pont szerint

„Magyarország a fizikai biztonságot veszélyeztető vagy jelentős anyagi károk okozására képes kiberképességeket fegyvernek, alkalmazásukat fegyveres agressziónak tekinti, amelyre a fizikai térben megvalósuló válaszadás is lehetséges. A kiberműveletek sokszor nehezen bizonyítható attribúciójára, az elkövető azonosítására, megnevezésére való tekintettel a válaszlépések különösen körültekintő, eseti elbírálást igényelnek az érintett kormányzati szervezetek bevonásával."

Ez a megfogalmazás teljes mértékben megegyezik a NATO, illetve az Európai Unió különböző szabályozásaival, doktrínáival, egyben kifejezi azt, hogy Magyarország is a kibertéri elrettentés stratégiáját követi, fölhíva a figyelmet minden ellenérdekelt ország számára, hogy egyrészt felkészülünk a válaszadásra, másrészt pedig szövetségeseinkkel együttműködve fogunk diplomáciai vagy akár katonai választ adni a magyar kiberteret érő bármilyen támadásra. Továbbmenve az alapvető érdekek felsorolásában, a 106. pontot kell még megemlíteni, mely szerint

„A forradalmi technológiák fejlesztése stratégiai fontosságú kérdés. Hazánk biztonsága megkívánja, hogy a kulcsfontosságú területeken – mint például a kibervédelem, a mesterséges intelligencia, az autonóm rendszerek, a biotechnológia – kiemelt figyelmet fordítsunk a kutatás-fejlesztésre és annak védelmi összetevőjére."

A védelmi innováció hangsúlyozása a magyar kormány számára évek óta kiemelten fontos, párhuzamosan a haderőnemi fejlesztésekkel, és ahogy a stratégiából kiolvasható, ebben a fejlesztésben a kibervédelemnek is kiemelt szerepe van. Ha ehhez hozzátesszük azt, hogy a mesterséges intelligencia is szerepel a felsorolt technológiák között, akkor egyértelműen következik, hogy a magyar állam tudomásul vette a mesterséges intelligencia alkalmazásának elkerülhetetlenségét, melynek következtében ezek a technológiák meg kell, hogy jelenjenek hazánk kibervédelmében is.

A Nemzeti Biztonsági Stratégia a kiemelt biztonsági kockázatok között, a 124. pontban fogalmazza meg a következőket:

„A változékony globális környezetben számos kihívás, kockázat és fenyegetés irányulhat hazánk vagy szövetségi rendszereink ellen. Magyarország Nemzeti Biztonsági Stratégiájában meghatározott értékeink és adottságaink alapján, az elemzett biztonsági környezetben a következő kihívások nemzeti érdekeinkre gyakorolt hatása a leginkább jelentős: (...)

d) jelentős károkat okozó kibertámadások a kormányzati informatikai rendszerek, az E-közigazgatás, a közműszolgáltatók, a stratégiai vállalatok, a létfontosságú infrastruktúra egyéb elemei és más, a társadalom működésében fontos szervezetek számítógépes hálózatai ellen..."

Elemezve ezt a pontot, továbbra is megerősítve láthatjuk, hogy Magyarország jellemzően államközpontú kibervédelem megvalósításában gondolkodik, egyrészt az állam számára fontos stratégiai adatok, másrészt pedig a kritikus infrastruktúrák védelme szerepel a kiemelt védendő területek között. Ahogy azt az egyéb releváns jogszabályokban is látni lehet, az adat, illetve az infrastruktúra védelmének együttes hangsúlyozása folyamatosan megjelenik. Az adat esetében a bizalmasság, a sértetlenség és a rendelkezésre állás, az infrastruktúra esetében a sértetlenség és a rendelkezésre állás biztosítása a kiemelten fontos feladat.

A stratégia 135. pontja határozza meg explicit módon a Magyar Honvédség kibertéri feladatkörét:

„135. A Magyar Honvédségnek jól felszerelt és jól kiképzett erőkkel, valamint rugalmas, hatékonyan alkalmazható, telepíthető és fenntartható, a szükséges mértékben interoperábilis képességekkel kell rendelkeznie, a mennyiségi mellett a minőségi mutatók javítására törekedve. Hagyományos országvédelmi és nemzetközi válságkezelési feladatai mellett egyaránt alkalmasnak kell lennie a tömeges bevándorlás okozta válsághelyzet, vagy a terrorveszély-helyzet kezeléséhez történő hozzájárulásra, a hibrid támadások elhárításában való szerepvállalásra, valamint a természeti vagy ipari katasztrófák következményeinek felszámolásában való közreműködésre. A haderőt úgy kell fejleszteni, hogy képes legyen hatásokat kiváltani a hazánk szempontjából releváns összes műveleti térben: a szárazföldön, a levegőben és a kibertérben egyaránt."

A kibertér mint a Magyar Honvédség számára fontos műveleti tér kiemelése jelzi azt is, hogy olyan képességeket kell fejleszteni, amelyek túlmennek korábbi képességein, és természetszerűleg ezeket a képességeket fel kell tudnia ajánlani a szövetségi rendszerben is. Ebben a pontban ki kell még emelni a hibrid fenyegetésekre való hivatkozást, hiszen ha együtt kezeljük a kibertérben, illetve az információs térben szereplő veszélyek együttesét, akkor jól érthető, hogy miért alakult át a Magyar Honvédség szervezeti rendszere 2019-től kezdődően, és jött létre az MH Kiber- és Információs Műveleti Központ, illetve miért konvergálnak egymáshoz a klasszikus információs műveletek, illetve a kibertéri katonai műveletek.

A stratégia az átfogó feladatok és eszközök felsorolása között a 159. pontban tovább elemzi a különböző teendőket, és így fogalmaz:

„A kibertérben jelentkező kihívások, kockázatok és fenyegetések kezelésére, a megfelelő szintű kiberbiztonság garantálására, a kibervédelmi feladatok ellátására, a nemzeti létfontosságú információs infrastruktúra zavartalan működésének biztosítására Magyarországnak készen kell állnia. Elsődleges feladat a kibertérben ténylegesen jelentkező vagy potenciális kihívások, kockázatok és fenyegetések azonosítása és nyomon követése, a kormányzati koordináció erősítése, a kibertér jogi szabályozásának fejlesztése, a felhasználók biztonságtudatos viselkedésének elősegítése, a kormányzati infokommunikációs rendszerek, a nemzeti létfontosságú információs infrastruktúra, a minősített információk és a nemzeti adatvagyon védelmének erősítése, valamint a kiberbiztonsággal kapcsolatos nemzetközi együttműködés bővítése. A katonai kibervédelmet növekvő mértékben alkalmassá kell tenni a haderő kinetikus műveleteinek kibertérbeli támogatására, ki kell alakítani a kiberműveletekben alkalmazható offenzív képességeket. Ennek érdekében fejleszteni kell a Magyar Honvédség kibervédelmi és kiberműveleti erőit."

Ez a pont gyakorlatilag keretbe foglalja Magyarország 2013-tól létrejövő információbiztonsági és kibervédelmi szabályozásait. Reflektál mindazokra a pontokra, melyek az egyes jogszabályokban megtalálhatóak, viszont újdonságként kiemeli a kiberműveletekben alkalmazható offenzív képességek megteremtésének szükségességét. A korábbi nemzeti szabályozás nem foglalkozott az offenzív képességek fontosságával, sőt, amikor a korábbi jogalkotási szakaszban előkerült az offenzív képességek fejlesztésének igénye, akkor a 2010-es években az ehhez szükséges politikai támogatást nem sikerült megszerezni. A 2020-as stratégia tehát jelentős eltérést mutat a korábbi gondolkodástól, és deklaráltan jelzi Magyarország ellenérdekelt országainak számára, hogy hazánk offenzív kibertéri képességével számolni kell.

A 160. pont szintén a nem állami szereplők bevonásának szükségességére hívja fel a figyelmet, akik nélkül a kiberképességek fejlesztése, az új technológiákhoz kapcsolódó innováció és ezek használatának elterjesztése elképzelhetetlen:

„Elengedhetetlen a nemzeti kibervédelmi képességek hazai bázisú kutatás-fejlesztéssel megalapozott erősítése, a korszerű technikai eszközök biztosítása. A kibervédelmi feladatok összetettsége miatt partnerséget kell kialakítani az állami és a magánszektor szereplői, az oktatási és a tudományos intézmények és az egyéni felhasználók között."

Ahogy arra is rávilágít a joganyag, hogy a nemzeti kibervédelem nemzetközi együttműködés nélkül nem működik. Ezt az együttműködést elsősorban a szövetségi rendszerben kell elképzelni, melynek alapja a bizalom kiépítése és megerősítése, oly módon, hogy akár politikai, akár technológiai szinten gyorsan és hatékonyan lehessen fellépni az országot érő kibertéri támadásokkal szemben.

„162. A kibertérrel kapcsolatos kihívások hatékony kezelése nemzetközi együttműködés nélkül elképzelhetetlen. Aktívan részt veszünk a globális kibertérben való felelős viselkedést szabályozó normák és a globális kiberbiztonság fokozására szolgáló

bizalomerősítő intézkedések kidolgozására és végrehajtására irányuló nemzetközi erőfeszítésekben."

A stratégia zárógondolata Magyarország biztonságának megteremtéséről is kiemeli a kibertér jelentette fenyegetések kezelését:

„175. A tömegpusztító fegyverek, a terrorizmus, a kibertámadások, a hibrid műveletek és a katasztrófák elleni védelem egyaránt megköveteli hazánk nemzeti ellenálló képességének fokozását."

2. A KIBERVÉDELEM SZAKPOLITIKAI SZINTJÉNEK HELYZETE ÉS KIHÍVÁSAI A NATO-BAN

A hidegháborút követően a NATO a 90-es évek végén, a 2000-es évek elején máris egy újabb kihívással került szembe, amely addig elképzelhetetlennek tűnt, még a szakembereknek is csak egy nagyon szűk köre volt, aki ezzel foglalkozott, erre próbálta felhívni a figyelmet. Ezek a számítógépes hálózatokat ért támadások, amelyeket ma kibertámadásoknak nevezünk, és amelyekkel a NATO elsőként az 1999-es koszovói bombázásokat követően szembesült leginkább. 1999. március 24-én, miután a NATO főtitkára bejelentette, hogy csapást mér a szerb célpontokra, megindultak az első kibertámadások a NATO ellen. A támadások alapvető célja a műveleti központ működésének zavarása, valamint a szövetségi honlapok elérhetetlenségének kiharcolása volt. Ezen túlmenően a támadásokért felelős szerb hackercsoport, a Fekete Kéz (Crna Ruka) politikai üzeneteket helyezett el több kormányzati weboldalon, valamint több alkalommal megpróbált betörni a szövetség parancsnoki szervereire, többnyire sikertelenül. Mindazonáltal sikeresen behatoltak a légierő számítógépes hálózatába, azonban ott nem tudtak hozzáférni semmilyen érzékeny információkhoz. Miután a belgrádi kínai nagykövetséget is bombatámadás érte, kínai és később orosz hackerek is csatlakoztak a támadókhoz, akik a jelentések szerint legalább 14 katonai és állami honlapot támadtak meg és tettek elérhetetlenné a balkáni háború alatt. Ezek a támadások viszonylag kisebb jelentőségűek voltak, súlyosságuk nem érte el azt a szintet, amikor ténylegesen átlépték volna azt a határt, ahol katonai kollektív védelemre lenne szükség.

A koszovói és az azt követő kiberincidensek azonban nagyban hozzájárultak ahhoz, hogy a döntéshozók felismerték a kibervédelem fontosságát. Ennek megfelelően a 2002-es prágai csúcstalálkozón kimondták, hogy a szövetségnek meg kell erősítenie a kibertámadások elleni védekezési képességeit, ami arra utal, hogy a szövetségesek ráébredtek a kibertámadások veszélyeire. Ezt erősíti meg az a tény is, hogy elindították a NATO kibervédelmi programját, amely magában foglalta a NATO számítógépes incidensekre való reagálási képességének (NATO Computer Incident Response Capability – NCIRC) kifejlesztését. Az e képesség mögött álló szervezet alapvető célja a NATO-rendszerekbe történő behatolások észlelése és szükség esetén a válaszadás.

Ezt követően a védelmi miniszterek 2007. június 14-i brüsszeli találkozóján a résztvevők a tagállamok kibervédelmi erőfeszítései egységesítésének szükségességére hívták fel a figyelmet. Ennek eredményeként a NATO 2008-ban új kibervédelmi irányelvet fogadott el e folyamatok összehangolása érdekében. Ennek kialakítását nagyban ösztönözte a 2007-ben történt átfogó kibertámadás-sorozat Észtország ellen, amelyben Európa egyik leginkább digitalizált országát támadták meg. A támadássorozat volt az első, amely megmutatta, hogy mit is eredményezhet pontosan egy kiberháború a valóságban, ami számos politikai és katonai vezetőt elgondolkodtatott, hogy komoly lépéseket kell tenni a területen.[4] Az egy évvel későbbi orosz–grúz konfliktus ismét rávilágított az információs műveletek, köztük a kiberhadviselés növekvő szerepére. A csúcstalálkozó során a NATO tisztviselői és kiberszakértők áttekintették az észtországi tapasztalatok tanulságait. A 2008-as bukaresti csúcstalálkozó vezetői nyilatkozatának 47. szakasza kimondta, hogy:

„47. A NATO továbbra is elkötelezett, hogy megerősítse a Szövetség kulcsfontosságú információs rendszereit a kibertámadásokkal szemben. Nemrég elfogadtuk a Kibervédelmi Irányelvet, és továbbra is fejlesztjük az ezt megvalósító szervezeteket és hatóságokat. A Kibervédelmi Irányelv hangsúlyozza, hogy a NATO-nak és a nemzeteknek is meg kell védeniük kulcsfontosságú informatikai rendszereiket saját felelősségi körükben; meg kell osztaniuk a legjobb gyakorlatokat és biztosítaniuk kell azokat a képességet, amelyekkel erre vonatkozó kérést követően egy szövetséges állam segítségére siethetnek egy kibertámadás elhárítására. Bízunk benne, hogy folytatódik a NATO kibervédelmi képességeinek fejlesztése és a kapcsolatok erősítése a NATO és a nemzeti hatóságok között."[5]

Mindezek eredményeképpen 2008 májusában létrejött a NATO Kooperatív Kibervédelmi Kiválósági Központ (NATO Cooperative Cyber Defence Centre of Excellence – CCDCOE), a NATO által akkreditált tudásközpont és képzési intézmény, amelynek fő feladata kutatások és fejlesztések, valamint konzultációk, képzések és gyakorlatok szervezése és lebonyolítása a kiberbiztonság területén, a nemzetközi katonai környezetre összpontosítva. A központ küldetése a képességek, az együttműködés és az információcsere fokozása a NATO, a szövetségesek és a partnerek között a kibervédelem területén.

A NATO a 2010-es lisszaboni csúcstalálkozón új stratégiai koncepciót fogadott el, amelynek során az Észak-atlanti Tanácsot (North Atlantic Council – NAC), a NATO legfőbb döntéshozó testületét megbízták egy alapos kibervédelmi politika kidolgozásával és az erre vonatkozó cselekvési terv elkészítésével. A dokumentum-

[4] Bányász Péter – Krasznay Csaba – Tóth András: A NATO kibervédelmi szakpolitikája. In Szenes Zoltán (szerk.): *A mai NATO. A szövetség helyzete és feladatai.* Budapest, HM Zrínyi Térképészeti és Kommunikációs Szolgáltató Nonprofit Kft., 2021, 130–149. o.

[5] Szentgáli Gergely: A NATO kibervédelmi politikájának fejlődése. *Bolyai Szemle,* 2012/2. szám, 80–85. o.

szövetség vezetői remélik, hogy a várva várt dokumentum megerősíti a transzatlanti köteléket, és felkészíti a NATO-t az új kihívások hatékony kezelésére. A csúcstalálkozón hozott döntésekkel kapcsolatban Jamie Shea főtitkárhelyettes a következőket mondta:

„Az új NATO-politika nemcsak azt teszi lehetővé, hogy a NATO gyorsabban és hatékonyabban védje saját hálózatait, hanem sokkal több segítséget nyújt a szövetségeseknek és a partnereknek a kiberbiztonság mindhárom kulcsfontosságú területén: megelőzés, a kibertámadások kezelése és hatásuk csökkentése, valamint a megtámadott országok segítése a létfontosságú információs rendszereik gyors visszaállításában és helyreállításában."

A csúcstalálkozót követően a tagállamok egy, a számítógépes rendszerek elleni támadások elhárítására összpontosító gyakorlatot tartottak Cyber Coalition 2010 néven. A gyakorlat során több tagállam és a főparancsnokság számítógépes rendszereit külső támadás érte, és a cél az volt, hogy a lehető leggyorsabban és legpontosabban azonosítsák az elkövetőket vagy a támadás eredetét. Az ilyen gyakorlatok mindenesetre hozzájárulnak a NATO kiberelhárítási képességeinek javításához, nem utolsósorban az elrettentés erősítéséhez.[6]

2011 júniusában a NATO védelmi miniszterei jóváhagyták a kibervédelemről szóló második NATO-irányelvet, amely a gyorsan változó fenyegetések és technológiai környezet összefüggésében egy szövetségen belüli összehangolt kibervédelmi erőfeszítésekre vonatkozó jövőképet fogalmazott meg. Ezt egy végrehajtási cselekvési terv kísérte. Az átdolgozott kibervédelmi irányelv a következő fő célokat tűzte ki:

- A kibervédelmi megoldások és elképzelések integrálása a NATO struktúráiba és tervezési folyamataiba a NATO kollektív védelemmel és válságkezeléssel kapcsolatos alapvető feladatainak ellátása érdekében.
- A NATO és a szövetségesek számára létfontosságú kibereszközök ellenálló képességére és védelmére, valamint a támadások megelőzésére való összpontosítás.
- Erős kibervédelmi képességek fejlesztése és a NATO saját hálózatai védelmének központosítása.
- A NATO alapvető feladatai szempontjából kritikus nemzeti hálózatok kibervédelmére vonatkozó minimumkövetelmények kidolgozása.
- Segítségnyújtás a szövetségeseknek a kibervédelem minimális szintjének eléréséhez és a nemzeti kritikus infrastruktúrák sebezhetőségének csökkentéséhez.
- Együttműködés a partnerekkel, nemzetközi szervezetekkel, a magánszektorral és a tudományos közösséggel.[7]

[6] Bányász Péter – Orbók Ákos: A NATO kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében. *Hadtudomány,* 2013/elektronikus szám, 188–209. o.

[7] NATO: *Defending the networks* (2011. augusztus 19.).

2012 áprilisára a kibervédelem is a NATO védelmi tervezési folyamatának részévé vált, így azóta a védelmi tervezési folyamatok keretében folyamatosan azonosítják és rangsorolják a vonatkozó kibervédelmi követelményeket. A 2012. májusi chicagói csúcstalálkozón a szövetséges vezetők megerősítették a szövetség kibervédelmének javítása iránti elkötelezettségüket azáltal, hogy a NATO összes hálózatát központosított védelem alá helyezték, és egy sor fejlesztést hajtottak végre az NCIRC – a NATO kibervédelmi képességének – tekintetében. Mindezekkel kapcsolatban a résztvevők az alábbiakat fogalmazták meg:

„49. A kibertámadások száma továbbra is jelentősen növekszik, és egyre kifinomultabbá és összetettebbé válnak. Megerősítjük a lisszaboni csúcstalálkozón tett kibervédelmi kötelezettségvállalásokat. Lisszabont követően tavaly elfogadtuk a kibervédelmi koncepciót, irányelvet és cselekvési tervet, amelyeket most hajtunk végre. A NATO meglévő képességeire építve 2012 végére létrejönnek a NATO számítógépes incidensekre való reagálási képességének (NCIRC) kritikus elemei, beleértve a legtöbb helyszín és felhasználó védelmét is. Kötelezettséget vállaltunk arra, hogy biztosítjuk a forrásokat és végrehajtjuk a szükséges reformokat, hogy valamennyi NATO-szervezetet központosított kibervédelem alá vonjuk, annak biztosítása érdekében, hogy a megerősített kibervédelmi képességek megvédjék a NATO-ba történő kollektív befektetésünket. A kibervédelmi intézkedéseket tovább fogjuk integrálni a szövetségi struktúrákba és eljárásokba, és mint egyes nemzetek, továbbra is elkötelezettek vagyunk a nemzeti kibervédelmi képességek azonosítása és megvalósítása mellett, amelyek erősítik a szövetségi együttműködést és interoperabilitást, többek között a NATO védelmi tervezési folyamatain keresztül. Továbbfejlesztjük a kibertámadások megelőzésére, felderítésére, az ellenük való védekezésre és az azokból való helyreállításra irányuló képességeinket. A kiberbiztonsági fenyegetések kezelése és közös biztonságunk javítása érdekében elkötelezettek vagyunk amellett, hogy a konkrét együttműködés fokozása érdekében eseti alapon együttműködjünk az érintett partnerországokkal, valamint nemzetközi szervezetekkel, többek között az EU-val – megállapodás szerint – az Európa Tanáccsal, az ENSZ-szel és az EBESZ-szel. Teljes mértékben ki fogjuk használni az észtországi Kooperatív Kibervédelmi Kiválósági Központ által kínált szakértelmet is."[8]

2012 júliusában a NATO ügynökségeinek reformja keretében létrehozták a NATO Kommunikációs és Információs Ügynökségét (NATO Communications and Information Agency – NCIA). Ezekkel a lépésekkel és intézkedésekkel a NATO elmélyítette a kapcsolatot más nemzetközi szervezetekkel, és elkezdődött az együttműködések kialakítása, amely nagymértékben hozzájárul a létfontosságú információs infrastruktúrák védelméhez.

2013-ban megjelent a Tallinni Kézikönyv (Tallinn Manual), amely alapvetően azokkal a kiberműveletekkel foglalkozik, amelyek sértik az erőszak alkalmazásának tilalmát, feljogosítják az államokat az önvédelem jogának gyakorlására, vagy fegy-

[8] NATO: *Chicago Summit Declaration* (2022. július 5.).

veres konfliktus során történnek, és elemzi a nemzetközi jog kiberhadviselésre való alkalmazásának köreit. Kiemeli az egyes elemzett esetek vonatkozásában az államok lehetséges szerepét, a nemzetközi humanitárius jog és a semlegesség jogának kérdéseit, továbbá a szuverenitást.

2014 februárjában a szövetséges védelmi miniszterek megbízták a NATO illetékes szervezeteit, hogy dolgozzanak ki egy új, továbbfejlesztett kibervédelmi politikát a kollektív védelem, a szövetségeseknek nyújtott segítség, az egységes kormányzás, a jogi megfontolások és az iparral való kapcsolatok tekintetében. Ennek eredményeképpen a 2014. szeptemberi walesi csúcstalálkozón a szövetségesek jóváhagyták a NATO új kibervédelmi irányelvét, és egy cselekvési tervet is, amely az irányelvvel együtt hozzájárul a szövetség alapvető feladatainak teljesítéséhez. A NATO kollektív védelemmel kapcsolatos alapvető feladatának részeként ismerték el a kibervédelmet, és a szövetségesek egyetértettek abban, hogy a kibertérben a nemzetközi jog alkalmazandó. Az ezt megfogalmazó nyilatkozat a kibervédelmet az átfogó védelmi csomag részévé tette, ami azt jelzi, hogy a NATO továbbra is komoly problémának tekintette a kiberfenyegetéseket, amelyek a kibertámadások elleni kollektív védekezést igénylik. A csúcstalálkozó nyilatkozata a továbbiakban megerősítette a kibővített kibervédelmi irányelvet:

„72. Ahogy a Szövetség a jövőbe tekint, a kiberfenyegetések és -támadások egyre gyakoribbá, kifinomultabbá és potenciálisan károsabbá válnak. E változó kihívással való küzdelem érdekében kiterjesztett kibervédelmi irányelvet fogadtunk el, amely hozzájárul a Szövetség alapvető feladatainak teljesítéséhez. A politika megerősíti a szövetségi biztonság, valamint a megelőzés, a felderítés, az ellenálló képesség, a helyreállítás és a védelem oszthatatlanságának elvét. Figyelmeztet arra, hogy a NATO alapvető kibervédelmi felelőssége saját hálózatainak védelme, és hogy a szövetségeseknek nyújtott segítséget a szolidaritás szellemével összhangban kell kezelni, hangsúlyozva a szövetségesek felelősségét a nemzeti hálózatok védelmére vonatkozó képességek kifejlesztésében. Irányelvünk azt is elismeri, hogy a nemzetközi jog, beleértve a nemzetközi humanitárius jogot és az ENSZ Alapokmányát, a kibertérben is alkalmazandó. A kibertámadások elérhetik azt a küszöböt, amely a nemzeti és euroatlanti jólétet, biztonságot és stabilitást veszélyezteti. Hatásuk ugyanolyan káros lehet a modern társadalmakra, mint egy hagyományos támadás. Ezért megerősítjük, hogy a kibervédelem a NATO kollektív védelmi alapfeladatának része. Arról, hogy egy kibertámadás mikor vezetne az 5. cikk alkalmazásához, az Észak-atlanti Tanács eseti alapon döntene."[9]

Ezzel először fogalmazták meg, hogy egy kibertámadás akár az 5. cikk hatálya alá is tartozhat, ennek megfelelően egy tagállam kibertérben történő megtámadása minden tagállam elleni támadásnak minősül, ennek megfelelően támogatni fogják a megtámadott felet vagy feleket akár fegyveres erő alkalmazásával is. Ebben a megfogalmazásban leginkább a kibertámadások hatásával foglalkoztak, és hogy a kiber-

[9] NATO: *Wales Summit Declaration* (2022. július 4.).

térben végrehajtott műveletek hatása megegyezhet a hagyományos támadásokéval. A walesi csúcstalálkozó döntései azt is megerősítették, hogy a kibervédelmi képességek fokozása érdekében tovább kell fejleszteni az ipari együttműködést, amellyel kapcsolatosan a NATO húsz területet határozott meg a kibervédelem minimális képességeinek fejlesztésével kapcsolatosan. Ezek közé a területek közé tartozik többek között a stratégiafejlesztés, az együttműködés, az oktatás és az információbiztonság.[10]

A 2012-es chicagói csúcstalálkozón elhangzottak megerősítéseképpen 2016. február 10-én a NATO és az EU technikai megállapodást kötött a kibervédelemről, amelynek alapvető célja, hogy mindkét szervezet hatékonyabban tudja megelőzni a kibertámadásokat, illetve jobban tudjon reagálni rájuk. Az NCIRC és az EU Számítógépes Vészhelyzeti Reagáló Csoportja (Computer Emergency Response Team for the EU – CERT-EU) közötti technikai megállapodás keretet biztosít az információcseréhez és a legjobb gyakorlatok megosztásához a vészhelyzeti reagáló csoportok (Emergency Response Team) között.

A 2016. júniusi varsói csúcstalálkozón a szövetséges állam- és kormányfők elismerték, hogy a kibertér olyan műveleti terület, amelyen a NATO-nak ugyanolyan hatékonyan kell védekeznie, mint a levegőben, a szárazföldön és a tengeren. Ez javította a NATO védelmi képességeit, amelyekkel kapcsolatosan a csúcstalálkozóról készített nyilatkozat a következőt mondja:

„70. A kibertámadások egyértelműen kihívást jelentenek a Szövetség biztonsága szempontjából, és ugyanolyan károsak lehetnek a modern társadalmak számára, mint a hagyományos támadások. Walesben megállapodtunk abban, hogy a kibervédelem része a NATO kollektív védelmi feladatainak. Most Varsóban megerősítjük a NATO védelmi mandátumát, és elismerjük a kiberteret olyan műveleti területnek, amelyben a NATO-nak olyan hatékonyan kell megvédenie magát, mint a levegőben, a szárazföldön és a tengeren. Ez javítani fogja a NATO azon képességét, hogy ezeken a területeken védje és végezze műveleteit, és minden körülmények között megőrizze cselekvési és döntéshozatali szabadságát. Továbbá támogatja a NATO szélesebb körű elrettentését és védelmét: a kibervédelem továbbra is beépül a működési tervezésbe és a Szövetség műveleteibe és küldetéseibe, és együtt fogunk dolgozni, hogy hozzájáruljanak a sikerhez. Ezenkívül biztosítja a NATO-kibervédelem hatékonyabb megszervezését és az erőforrások, készségek és képességek jobb kezelését. Ez a NATO hosszú távú alkalmazkodásának része. Továbbra is végrehajtjuk a NATO-nak a kibervédelemre vonatkozó továbbfejlesztett politikáját, és megerősítjük a NATO kibervédelmi képességeit, kihasználva a legújabb élvonalbeli technológiákat."[11]

[10] Bányász Péter: *A közösségi média lehetőségei és kihívásai a védelmi szférában*. Doktori (PhD) értekezés, Budapest, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola 2018.

[11] Paráda István: A NATO kibervédelmi irányelveinek fejlődése. *Honvédségi Szemle*, 2018/3. szám. 3–13. o.

Mindez azt mutatja, hogy a vezetők célul tűzték ki a kibervédelem javítását, annak nagyobb mértékű integrálását a tervezési folyamatokba, valamint a nemzeti és szövetséges hálózatok védelmének fokozását a legmodernebb technológiák alkalmazásával. Varsóban mindezek mellett elfogadtak egy Kibervédelmi Vállalást (Cyber Defence Pledge) is, amelyben nyilatkoztak arról, hogy jelentősen fejleszteni fogják nemzeti hálózataik és infrastruktúráik védelmét. Ennek megfelelően kötelezettséget vállaltak arra, hogy a védelmi szervezetekben kiépítik a kibervédelmi képességek teljes skáláját, megfelelő forrásokat különítenek el a nemzeti szintű képességfejlesztésre, elmélyítik a fenyegetések és védelmi tevékenységek azonosítására és értelmezésére irányuló együttműködést, valamint fokozzák a kibervédelmi oktatást és képzést. Ezekkel egyidejűleg a 2014-es walesi csúcstalálkozót követően a varsói csúcstalálkozón a vezetők megerősítették a kollektív védelem kibertérre történő kiterjesztésére tett döntésüket, ezzel hivatalosan is deklarálva azt.[12]

2017 februárjában a szövetséges védelmi miniszterek jóváhagyták a kibervédelmi cselekvési terv aktualizált változatát, valamint a kibertér mint műveleti terület megvalósításának ütemtervét. Ez nagymértékben hozzájárult a szövetségesek együttműködési képességének, a képességek fejlesztésének és az információmegosztás lehetőségeinek növeléséhez. Ebben az évben jelent meg a Tallinni Kézikönyv 2.0, amely a nemzetközi jog azon szabályait vizsgálja, amelyek az államok által nap mint nap tapasztalt, de az erő alkalmazásának vagy a fegyveres konfliktusnak a küszöbértékét el nem érő kiberincidensekre vonatkoznak. A szuverenitás és az állami felelősség mellett olyan kérdésekkel is foglalkozik, mint az emberi jogok, valamint a levegő, a világűr és a tenger joga.

A 2018-as brüsszeli csúcstalálkozón a szövetséges vezetők megállapodtak abban, hogy tovább optimalizálják a NATO hírszerzési tevékenységeit, hogy elősegítsék a szövetséges döntéshozatalt és a műveletek időben történő és releváns támogatását, többek között a riasztások és a hírszerzési információk megosztásának javítása révén, különösen a terrorizmussal, a hibrid és a kibertérrel kapcsolatban. Kimondták, hogy a NATO továbbra is alkalmazkodni fog a folyamatosan változó kiberfenyegetettségekhez, amelyeket állami és nem állami szereplők egyaránt befolyásolhatnak. A csúcsértekezleten hozott döntések alapján Belgiumban az európai műveleti parancsnokságon belül (SHAPE) létrehoztak egy kibertérműveleti központot (Cyber Operational Center – CyOC), amely a NATO kibertéren belüli operatív tevékenységének helyzetfelismerését és koordinálását biztosítja.[13]

A 2019-es londoni csúcstalálkozón is szintén több kibervédelmet érintő döntés született. Megállapodtak abban, hogy növelik a kibertámadásokra reagáló eszközök

[12] Berki Gábor: *Kiberháborúk, kiberkonfliktusok. Műhelymunkák.* Budapest, Geopolitikai Tanács Közhasznú Alapítvány, 2016, 245–284. o.

[13] Mitko Bogdanoski: Building Cyber Resilience against Hybrid Threats. *NATO Science for Peace and Security Series – D: Information and Communication Security*, 2022.

és képességek számát, ezáltal erősítik a biztonságot a szövetségen belül, valamint felkészülnek a társadalmat veszélyeztető hibrid fellépésekre, megfelelő védelmi megoldásokat dolgoznak ki, valamint alkalmazzák az elrettentés módszerét. Elhangzott, hogy a NATO és a szövetségesek elkötelezettek amellett, hogy saját területükön megerősítsék a kommunikáció biztonságát, beleértve az 5G-t is, felismerve, hogy a feladatok végrehajtása során minden körülmények között biztonságos és rugalmas kommunikációs rendszerekre kell támaszkodni. A csúcstalálkozó másik eredménye, hogy a NATO a világűrt műveleti dimenzióvá nyilvánította, felismerve annak fontosságát biztonságunk megőrzésében és a biztonsági kihívások kezelésében, a nemzetközi jog tiszteletben tartása mellett.[14] Az NCIA még ebben az évben megkezdte a Kiberbiztonsági Együttműködési Központ (Cyber Security Collaboration Hub) létrehozását, amely a tagállamok számára egy titkos információgyűjtési, együttműködési és képzési platformot biztosít. Az NCIA korábban is szolgáltatott információkat a szövetséges nemzeti számítógépes vészhelyzeti reagáló csoportok (CERT) részére, de NATO CERT-közösség nem létezett.

Az Észak-atlanti Tanács 2020. június 3-án kiadta nyilatkozatát a rosszindulatú kibertevékenységekről (North Atlantic Council Statement on Malicious Cyber Activities 2020), amelyben elítélte a destabilizáló és rosszindulatú kibertevékenységeket a koronavírus világjárvánnyal összefüggésben. A NATO-nyilatkozat szolidaritásáról és kölcsönös támogatásáról biztosította a rosszindulatú kibertevékenységek által érintetteket, köztük az egészségügyi szolgálatokat, kórházakat és kutatóintézeteket. A nyilatkozat a nemzetközi jog és a felelős állami magatartás normáinak tiszteletben tartására szólított fel a kibertérben, miután a Kínából vagy Oroszországból irányított dezinformációs kampányok elárasztották a nyugati médiát és a közösségi hálózatokat.[15]

A 2021. júniusi brüsszeli csúcstalálkozón a szövetségesek elismerték a változó fenyegetettségi környezetet, felismerve, hogy a kibertér folyamatos támadásoknak van kitéve. A szövetségesek új, átfogó kibervédelmi irányelvet hagytak jóvá, amely támogatja a NATO három alapvető küldetését, a kollektív védelmet, a válságkezelést és a kooperatív biztonságot, valamint hozzájárul a NATO általános elrettentő és védelmi pozíciójának fenntartásához. A NATO-nak mindenkor – békeidőben, válságban és konfliktusban – politikai, katonai és technikai szinten is aktívan elrettentenie, védenie és elhárítania kell a kiberfenyegetések teljes spektrumát.

A CCDCOE a közelmúlt kibernetikai eseményeire és konfliktusaira reflektálva 2022-ben közzétette a Kibertér stratégiai kilátások 2030 (Cyberspace Strategic Outlook 2030) című dokumentumát. A kiadvány a NATO kiberfenyegetésekre adott

[14] NATO: *London Declaration*. (2022. július 1.).

[15] Dragoş-Mihai Păunescu: NATO's encounters in the cyber domain. *Proceedings of the 17th International Scientific Conference „Strategies XXI" – Strategic Changes in Security and International Relations*, 2021/1. szám.

válaszaira összpontosít a 2022–2030-as időszakban, kitérve az új és átalakuló technológiákra, a fejlődő kiberfenyegetésekre, a kibertér szereplőinek stratégiáira és tevékenységeire, valamint a változások egyéb mozgatórugóira. Elemzi és értékeli, hogyan lehet a Szövetséget katonailag és politikailag megerősíteni a kiberfenyegetésekkel szemben.[16]

A NATO saját elemzései és dokumentumai alapján összességében úgy fogalmaz, hogy míg minden egyes szövetséges fél felelős a saját kibervédelméért, a NATO platformként szolgál a szövetségesek számára, hogy konzultáljanak kibervédelmi kérdésekről, megosszák a kiberfenyegetésekkel kapcsolatos információkat, kicseréljék a legjobb gyakorlatokat, és összehangolják a tevékenységeiket. A NATO támogatja tagjait a kibervédelem megerősítésében, például a következőkkel:

- A fenyegetésekkel kapcsolatos valós idejű információk megosztásával egy külön erre a célra létrehozott, rosszindulatú szoftverekkel kapcsolatos információmegosztó platformon (malware information sharing platform – MISP) keresztül, valamint a kiberfenyegetésekre való reagálásra vonatkozó legjobb gyakorlatok cseréjével;
- Gyorsreagálású kibervédelmi csapatok fenntartásával, amelyeket a szövetségesek segítségére lehet küldeni a kibertérben jelentkező problémák kezelése céljából;
- A szövetségesek számára célok kidolgozásával a kibervédelmi képességeik közös megközelítésének megkönnyítése érdekében;
- Az oktatásba, képzésbe és gyakorlatokba való befektetéssel, mint például a Cyber Coalition, az egyik legnagyobb kibervédelmi gyakorlat a világon.

A szövetségesek nemzeti felelősségeikkel és hatáskörükkel összhangban elkötelezettek a kritikus infrastruktúrájuk védelme, az ellenálló képesség kiépítése és a kibervédelem megerősítése mellett, többek között a NATO kibervédelmi vállalásának teljes körű végrehajtása révén.[17]

3. A KIBERVÉDELEM SZAKPOLITIKAI SZINTJÉNEK HELYZETE ÉS KIHÍVÁSAI AZ EURÓPAI UNIÓBAN

A NATO kiberbiztonsági stratégiájának fejlődése mellett fontos az Európai Unió ez irányú stratégiaalkotási folyamatának vizsgálata is, már csak azért is, hiszen jelentős előzményei azoknak az európai jogszabályoknak, amik az adat-, információ- és hálózatbiztonság szempontjából Magyarország normatív szabályozási környezetében is szerepet kap. A helyzetet nehezítik az Európai Unió jogalkotásának, illetve állam-

[16] Piret Pernik (szerk.): *Cyberspace Strategic Outlook 2030.* Tallinn, CCDCOE, 2022.
[17] NATO: *Fact Sheet – NATO Cyber Defence* (2021. április 28.).

szerkezetének sajátosságai. Visszatérő vita többek között, hogyan is kell értelmezni az EU-t, konföderációnak, föderációnak, az általa meghozott normatív szabályozók az egyes tagállamokra milyen kötelezettségeket rónak. Az EU-val kapcsolatos tanulmányok kiinduló tétele az úgynevezett „spill over" hatás, ami nagyon leegyszerűsítve azt az elvet írja le, egy valamilyen szakpolitikára vonatkozó szabályozás gyakran más szakterületekre is „továbbgyűrűzik". Esetünkben ez azért fontos, mert a kiberbiztonság egy rendkívül összetett szakterület, ami – ahogy a Nemzeti Kiberbiztonsági Stratégia is megfogalmazza – „*kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez*". E fogalomból következik, hogy az Európai Unió számos területen igyekszik normatív szabályokat alkotni.

Az Európai Unió már az 1990-es évek közepén felismerte, hogy az elektronikus információs rendszereinek védelme fontos feladat (elsősorban a telekommunikációs rendszerek és a személyes adatok védelme aspektusából),[18] de stratégiai szinten először 2006-ban jelent meg hivatalos dokumentum a kiberbiztonsággal kapcsolatban Biztonságos információs társadalom elnevezéssel.[19]

A 2007-ben Észtország kormányzati és pénzügyi kritikus infrastruktúráit ért több túlterheléses támadás nem csupán a NATO esetében volt fontos jelzés a terület mielőbb szabályozása okán, hanem az Európai Uniónak is. A 2008-ban kitört gazdasági és pénzügyi válság, a kibertérből származó fenyegetéseknek, különösen a kiberbűnözés nagyarányú növekedése az EU döntéshozói számára is világossá tette, hogy a kibertérből származó új típusú kihívásokra erőteljes választ kell adni. Az azóta eltelt időszakban az EU számos különböző stratégiai dokumentumot fogadott el, amelyek részletes bemutatását e fejezet terjedelmi keretei nem teszik lehetővé, csupán a meghatározóbb történeti előzmények felvillantására nyílik alkalmunk. Ez a megkötés ugyanúgy érvényes a jelenleg elfogadás alatt álló stratégiákra is, ugyanis az említett komplexitásból fakadóan meglátásunk szerint nem értelmezhető önmagában a „kiberbiztonság", csak ökoszisztémában rendezve.

A történeti áttekintés alapján az első említendő dokumentum az Európa 2020 foglalkoztatási és növekedési stratégia,[20] amely a 2020-ig tartó időszak intézkedései alapdokumentumának tekinthető. Ennek keretében az Európai Bizottság hét kiemelt szabályozási területet azonosított, aminek a megvalósítása érdekében elkészí-

[18] Helena Carrapico – Andre Barrinha: European Union cyber security as an emerging research and policy field. *European Politics and Society,* 2018/3. szám, 299–303. o.

[19] E dokumentum előzményeként meg kell említenünk a Hálózat- és információbiztonság: európai politikai megközelítésre irányuló javaslatot [COM(2001)] 2001-ből.

[20] Európa 2020 – Az intelligens, fenntartható és inkluzív növekedés stratégiája.

tette az Európai Digitális Menetrend 2014–2020 stratégiáját.[21] Az Európai Digitális Menetrend többek között az alábbi megvalósulását tűzte ki:

- *az egységes digitális piac megteremtése,*
- *az uniós adatvédelmi szabályozási keret felülvizsgálata,*
- *a távközlési szolgáltatások egységesítése,*
- *a fokozott interoperabilitás és szabványok.*[22]

Következő lépésként az Európai Parlament, a Tanács, az Európai Gazdasági és Szociális Bizottság és a Régiók Bizottsága által 2013-ban megalkotott az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér című uniós stratégiáját nevesíthetjük. A stratégia hat stratégiai prioritást és intézkedést fogalmazott meg.[23]

2018. május 25-étől az Európai Unió tagállamaiban egységesen az Európai Általános Adatvédelmi Rendelet lépett hatályba,[24] és a GDPR rendelkezéseit kell alkalmazni tagállamokban korábban hatályos adatvédelmi szabályok helyett. A Rendelet alapjául az Európai Parlament és a Tanács 95/46/EK irányelve szolgált.[25] Bár az irányelv rögzítette a személyes adatok kezelésének elveit, azonban nem határozta meg az adatvédelmi incidensek megsértésének következményeit. Az új adatvédelmi rendelet egyrészt a hiátust pótolja, másrészt egységes követelményrendszert fogalmaz meg a személyes adatok kezelését illetően az Európai Unió minden tagállamában, továbbá korszerű választ kíván adni a technológiai fejlődésből következő kockázatokra, hogy ennek segítségével növekedjen a felhasználók új technológiákba vetett hite, és ezáltal növekedhessen a Digitális Menetrendben megfogalmazott európai digitális tér.

A GDPR mellett fontos változást jelentett a szintén 2018 májusától érvényes hálózati és információs rendszerek biztonságáról szóló irányelv (Az Európai Parlament és a Tanács [EU] 2016/1148 irányelve [2016. július 6.] a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító in-

[21] Európai Digitális Menetrend 2010–2020: A Bizottság akcióterve az európai jólét fellendítésére.

[22] A témáról bővebben lásd Munk Sándor: Kiberbiztonsági célok, jövőképek, szabályozók az EU-ban és kapcsolatrendszerük az interperabilitással. *Hadmérnök,* 2018/KÖFOP szám, 205–217. o.

[23] Közös közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér, text/html; charset=UTF-8 (OPOCE).

[24] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (EGT vonatkozású szöveg).

[25] Az Európai Parlament és a Tanács a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK irányelve.

tézkedésekről, továbbiakban NIS-irányelv).[26] A NIS-irányelv megalkotásának előzményei az európai stratégiai fejlődésre vezethetőek vissza. Az irányelv célja, hogy az EU tagállamai képesek legyenek a kibertér jelentette fenyegetések ellen hatékonyan védekezni, ily módon pedig létrejöjjön egy egységes hálózati és információs rendszerek biztonságára vonatkozó, általános uniós szint.

Mivel irányelvként fogadták el a jogszabályt, így a tagállami jogalkotók maguk határozhatják meg, hogy milyen módon implementálják az irányelvben megfogalmazottakat a tagállami joganyagokba. 2022 májusában a Tanács és az Európai Parlament végül elfogadta a NIS2-irányelvet,[27] ami a 2018-ban hatályba lépett irányelv újragondolása. A módosított irányelv célja, hogy *„megszüntesse azokat az eltéréseket, amelyek jelenleg a különböző tagállamokban mutatkoznak a kiberbiztonsági követelmények és a kiberbiztonsági intézkedések végrehajtása terén. Ennek érdekében minimumszabályokat állapít meg a szabályozási keretre vonatkozóan, és mechanizmusokat határoz meg az egyes tagállamok illetékes hatóságai közötti hatékony együttműködéshez. Aktualizálja a kiberbiztonsági kötelezettségek hatálya alá tartozó ágazatok és tevékenységek listáját, és a végrehajtás biztosítása érdekében jogorvoslatokról és szankciókról rendelkezik."*

2019 áprilisában a Tanács elfogadta a Kiberbiztonsági jogszabályt, ami bevezeti az egész Unió területén érvényes egységes kiberbiztonsági tanúsítási rendszerek keretét, illetve létrehozza az Európai Hálózat- és Információbiztonsági Ügynökség feladatainak átvételére az az Európai Uniós Kiberbiztonsági Ügynökséget. A tanúsítási keretrendszer a tervek szerint növelni fogja a bizalmat, fokozza a kiberbiztonsági piac növekedését, valamint megkönnyíti e termékek EU-n belüli kereskedelmét.[28]

2020 februárjában kezdődött meg az Európai Unió digitális jövőjének megtervezése, amely ötéves intervallumban három fő célkitűzést fogalmazott meg:

- az emberek szolgálatában álló technológia;
- a méltányos és versenyképes gazdaság; valamint
- a nyílt, demokratikus és fenntartható társadalom.

E jövőkép pilléreiként az európai adatstratégiát, a kommunikációt biztosító keretrendszert, valamint a mesterséges intelligencia használatára vonatkozó fehér könyvet azonosították. A 2019 végén kitört új típusú koronavírus-járvány (továbbiakban Covid19) miatt újratervezés vált szükségessé, ami a NextGeneration EU formájában valósult meg a Bizottság 2020. májusi előterjesztése alapján.[29] A koncepció célja, hogy a Covid19 okozta társadalmi és gazdasági nehézségeket követően a helyreállí-

[26] Az Európai Parlament és a Tanács a hálózati és információs rendszereknek az egész unióban egységesen magas szintjét biztosító intézkedésekről szóló 2016/1148 irányelve.

[27] A kiberbiztonság és -reziliencia megerősítése az EU egész területén – Ideiglenes megállapodás a Tanács és az Európai Parlament között.

[28] The EU Cybersecurity Certification Framework | Shaping Europe's Digital Future.

[29] Bővebben lásd Európai helyreállítási terv, Text, Európai Bizottság – European Commission.

tás valamennyi tagállam számára fenntartható, méltányos, inkluzív és egyenletes legyen. Mindennek egyik eszközeként a digitalizáció erősítését nevesítették, ideértve:

- az 5G hálózatok gyors kiépítését;
- az ipari és technológiai jelenlét fokozását a stratégiai ágazatokban (nevesítve a mesterséges intelligenciát, a kvantum számítástechnikát, illetve a felhőalapú számítástechnikát);
- az innováció és a munkahelyteremtés motorjaként szolgáló valódi adatgazdaság kiépítése, illetve a kiberrezilencia növelését.

2020 szeptemberében hirdette meg a Bizottság az EU Digitális évtizedét. A megfogalmazott ajánlásokban tovább erősödött az 5G hálózatok mielőbbi kiépítésének (kiemelve a hálózatok biztonságának és ellenálló képességének növelését, illetve az Európai Unió Kiberbiztonsági Ügynökségével együttműködve erre vonatkozó stratégia megalkotását), a kvantumszámítástechnika területén történő fejlesztések szükségessége.[30]

Szintén szeptemberben nyújtotta be a Bizottság a Digitális pénzügyi csomag javaslatát, amelynek két javaslatát végül a Tanács 2021 novemberében fogadta el. E két javaslat a kriptoeszközök piacairól szóló rendeletjavaslat (MiCA-rendelet), valamint a digitális működési rezilienciáról szóló rendeletjavaslat (DORA-rendelet). A MiCA-rendelet célja, hogy olyan szabályozási keretet hozzon létre a kriptoeszközök piaca számára, amely támogatja az innovációt, és kiaknázza a kriptoeszközökben rejlő lehetőségeket, ugyanakkor biztosítja a pénzügyi stabilitás és a befektetők védelmét. A DORA-rendelet célja a digitális működési rezilienciára vonatkozó, olyan szabályozási keret létrehozása, amelynek értelmében valamennyi vállalkozás gondoskodik arról, hogy a kiberfenyegetések megelőzése és enyhítése érdekében ki tudja védeni az IKT-vonatkozású zavarokat és fenyegetéseket.[31]

2020 decembere különösen jelentős volt az Európai Unió stratégiaalkotásában. A Tanács következtetést fogadott el a csatlakoztatott eszközök kiberbiztonságáról, amely a dolgok internetéhez (IoT) kapcsolódó legmagasabb szintű reziliencia megteremtését fogalmazta meg annak céljából, hogy előrelendítse az EU IoT ágazatának globális versenyképességét.[32]

[30] A Tanács végül 2021 júliusában fogadta el az európai nagy teljesítményű számítástechnikával foglalkozó közös vállalkozás (EuroHPC közös vállalkozás) létrehozásáról szóló rendeletet. Bővebben lásd Európai nagy teljesítményű számítástechnikával foglalkozó közös vállalkozás: a Tanács rendeletet fogadott el.

[31] Digitális pénzügyi csomag: a Tanács megállapodásra jutott a MiCA- és a DORA-rendeletről (https://www.consilium.europa.eu/hu/press/press-releases/2021/11/24/digital-finance-package-council-reaches-agreement-on-mica-and-dora/).

[32] A Tanács következtetéseket fogadott el a csatlakoztatott eszközök kiberbiztonságáról (https://www.consilium.europa.eu/hu/press/press-releases/2020/12/02/cybersecurity-of-connected-devices-council-adopts-conclusions/).

Szintén említendő a Tanács által e hónapban közzétett állásfoglalás a titkosítással kapcsolatban. Az állásfoglalás nagy vitát generált a szakemberek között, ugyanis bár kimondja, hogy a titkosítással védeni kell a kommunikáció biztonságát, ennek ellenére garantálni szükséges a biztonságot is, amely a bűnüldöző és igazságügyi hatóságok részére biztosítaná, hogy az online és offline térben gyakorolni tudják jogszerű hatásköreiket.[33]

December 15-én terjesztette be a Bizottság az egyik legjelentősebb reformcsomagját a digitális tér átfogó megújítására vonatkozóan. E csomag két jelentős jogszabályt tartalmazott, a Digitális Szolgáltatásokról szóló (Digital Service Act, DSA), illetve a Digitális Piacról szóló Jogszabályt (Digital Market Act, DMA). A DSA célja, hogy az európai értékekkel összhangban védje a felhasználókat és azok jogait az online térben, ami alapján szilárd keretet alakít ki az online platformok átláthatóságának és elszámoltathatóságának biztosítása érdekében. A digitális szolgáltatásokról szóló jogszabály értelmében uniós szintű, kötelező érvényű kötelezettségek vonatkoznak majd minden olyan digitális szolgáltatásra, amelyek árukat, szolgáltatásokat vagy tartalmakat közvetítenek a fogyasztóknak. A jogszabály többek között olyan új eljárások bevezetését javasolja, amelyeknek alapvető célja az illegális tartalmak eltávolításának felgyorsítása az online platformokról, továbbá a felhasználók alapvető online jogai általános védelmének fokozása.[34] A DMA célja, hogy a nagy technológiai cégek (az EU terminológiájában digitális kapuőrök) működését szigorúbb jogi keretek szabályozzák.[35] A jogszabály várhatóan 2023 tavaszán lép hatályba.

E két jogszabály mellett a Tanács következtetéseket is elfogadott a reziliencia erősítésére, a hibrid fenyegetésekkel szembeni ellenálló képesség növelésére, kiemelten kezelve a dezinformációt, ami a Covid19 járvány következtében különösen relevánssá vált.[36] A globális dezinformációs kampányok mögött gyakran az Európai Unió stratégiai ellenfelei állnak azzal a céllal, hogy ily módon csökkentsék a demokratikus intézményekbe, a tudományba vetett bizalmat, illetve dezintegrálják az Uniót, megosszák az egyes tagállamokat. Ezek a tendenciák a 2022. február 24-én

[33] Titkosítás: a Tanács állásfoglalást fogadott el (https://www.consilium.europa.eu/hu/press/press-releases/2020/12/14/encryption-council-adopts-resolution-on-security-through-encryption-and-security-despite-encryption/).

[34] A jogszabályt 2022 júliusában fogadta el az Európai Parlament, jelenleg a Tanács jóváhagyása szükséges a hatálybalépéshez. Bővebben lásd „A digitális szolgáltatásokról szóló jogszabálycsomag", Text, European Commission – European Commission, elérés (https://ec.europa.eu/commission/presscorner/detail/hu/IP_22_4313).

[35] A jogszabályról bővebben lásd A digitális piacokról szóló jogszabály: tisztességes és nyitott digitális piacok biztosítása, Text, European Commission – European Commission (https://ec.europa.eu/commission/presscorner/detail/hu/qanda_20_2349).

[36] A Tanács a reziliencia megerősítésére és a hibrid fenyegetések, többek között a dezinformáció elleni küzdelemre szólított fel (https://www.consilium.europa.eu/hu/press/press-releases/2020/12/15/council-calls-for-strengthening-resilience-and-countering-hybrid-threats-including-disinformation-in-the-context-of-the-covid-19-pandemic/).

kitört ukrán–orosz háborút megelőzően, és azt követően, különösen a szankciók bevezetése okán még intenzívebbé váltak.

Egy nappal később a Bizottság a csomag részeként az Unió új kiberbiztonsági stratégiáját is benyújtotta. A stratégia célja kiberfenyegetésekkel szembeni rezilienciája, valamint hogy minden polgár és vállalkozás megbízható szolgáltatásokat és digitális eszközöket vehessen igénybe, és ezek előnyeit teljes mértékben ki tudja használni. Végül a 2021. március 22-én következtetéseket fogadott el a Tanács a kiberbiztonsági stratégiáról, amelyekben hangsúlyozta, hogy a kiberbiztonság alapvető fontosságú a reziliens, zöld és digitális Európa építésében.[37] A Digitális Évtized új kiberbiztonsági stratégiája nagyban támaszkodik a fejezetben említett, a kiberbiztonságra vonatkozó ellenálló képesség erősítését szorgalmazó dokumentumokra, illetve a biztonsági unióra vonatkozó stratégiára. A stratégia az alábbi területeken fogalmaz meg konkrét intézkedési javaslatokat:

- reziliencia, technológiai szuverenitás és vezető szerep;
- operatív kapacitás kiépítése: a megelőzés, elrettentés és reagálás elősegítése;
- a globális és nyitott kibertér kiépülésének és működésének támogatása.

A Tanács által elfogadott következtetések az új kiberbiztonsági stratégia kapcsán az alábbi intézkedési területeket jelölte meg:

- kiberbiztonsági műveleti központok hálózatának kiépítése a hálózatok monitorozására és a támadások korai előrejelzésére;
- közös uniós kiberbiztonsági egység létrehozása a kiberbiztonsági válsághelyzetek hatékony kezelésére;
- közös uniós 5G eszközkészlet kialakítása az 5G hálózatok kiberbiztonsági védelmének biztosítására;
- közös uniós internetbiztonsági szabványok bevezetése, mivel ezek kulcsfontosságúak a kibertér biztonságának elősegítésében, miközben a globális internetes hálózatok nyitottságát is szolgálják;
- az erős titkosítás eljárásai kifejlesztésének támogatása az alapvető állampolgári jogok és a digitális biztonság megőrzésére;
- az EU kiberdiplomáciai eszközkészletének továbbfejlesztése, a kibertámadások megelőzésének és elhárításának elősegítésére;
- egy közös uniós kiberhírszerzési munkacsoport felállítása az EU általános célú hírszerző szervezetének (EU INTCENT) megerősítésére;
- multilaterális együttműködések erősítése a kiberbiztonság és kibervédelem területén;

[37] Kiberbiztonság: a Tanács következtetéseket fogadott el az uniós kiberbiztonsági stratégiáról (https://www.consilium.europa.eu/hu/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy/).

- az Unió kiberbiztonsági kapacitásépítő tevékenységének kiterjesztése az EU-n kívüli területekre annak érdekében, hogy a kibertámadásokkal szembeni ellenálló képesség világszerte növekedhessen.

Fentiekhez igazodik a Bizottság 2021. márciusi előterjesztése, a 2030-as időszakig vonatkozó Digitális iránytű: A digitális évtized európai útja nevet viselő dokumentum, ami digitálisan képzett lakosság és magasan képzett digitális szakemberek, biztonságos, jól teljesítő és fenntartható digitális infrastruktúrák, a vállalkozások digitális átalakítását és a közszolgáltatások digitalizálását tűzte ki céljául.

Említeni szükséges a stratégiai fejlődés tekintetében a Mesterséges Intelligenciarendszerek fejlesztése és alkalmazása az Európai Unióban nevet viselő tervezetet, aminek elsődleges célja, hogy megóvja az Európai Uniót egy MI alapú disztópikus rendszer kialakulásától. A szabályozással egy, a kínai szociális kreditrendszerhez hasonló, totális megfigyelő állam kialakulásának lehetőségét szeretnék elérni. Az ily módon kialakítandó keretrendszer a MI-rendszerek fejlesztését és alkalmazását kockázatelemzéshez kötné, amelyben elfogadhatatlan, magas, korlátozott, illetve minimális kockázatot jelentő kategóriák mentén szabályozná a kérdéskört.

A bemutatott stratégiák mellett említeni szükséges Európai Kiberbiztonsági Kutatási és Kompetenciaközpont létrehozásával kapcsolatos szakpolitikai fejlődést. A szervezet megalakítását 2020 decemberében jelentették be bukaresti székhellyel. A központ feladata, hogy javítsa a kiberbiztonsági kutatások és innováció koordinációját az EU-ban.[38]

Ahogy a Covid19 járvány, úgy az említett ukrán–orosz háború kitörése is új szabályozási környezet kialakításának igényét hozta el. 2022 márciusában uniós tagállamok távközlésért és digitális ügyekért felelős miniszterei a kiberbiztonság területén folytatott európai együttműködés megerősítésére és ütemének felgyorsítására szólítottak fel a szomszédban zajló háború okán.[39]

Májusban a Tanács további három évvel hosszabbította meg az Uniót és annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedések keretének érvényességét.[40] A bevezethető szankciók előzménye a 2017-ben megalkotott Kiberdip-

[38] A Tanács zöld utat adott a bukaresti székhelyű Kiberbiztonsági Kompetenciaközpont létrehozásának (https://www.consilium.europa.eu/hu/press/press-releases/2021/04/20/bucharest-based-cybersecurity-competence-centre-gets-green-light-from-council/).

[39] Member States United in Supporting Ukraine and Strengthening the EU's Telecommunications and Cybersecurity Resilience – French Presidency of the Council of the European Union 2022, French Presidency of the Council of the European Union (http://presidence-francaise.consilium.europa.eu/en/news/member-states-united-in-supporting-ukraine-and-strengthening-the-eu-s-telecommunications-and-cybersecurity-resilience/).

[40] Kibertámadások: a Tanács 2025. május 18-ig meghosszabbította a szankciórendszer érvényességét (https://www.consilium.europa.eu/hu/press/press-releases/2022/05/16/cyber-attacks-council-extends-sanctions-regime-until-18-may-2025/).

lomáciai eszköztár a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretét határozza meg. Néhány nappal később a Tanács következtetéseket fogadott el a kiberreziliencia erősítésére vonatkozóan.[41]

A háború okán júniusban a hibrid hadjáratokra való koordinált uniós reagálásra vonatkozó következtetéseket fogadott el a Tanács,[42] amiben ismételten hangsúlyozta, hogy bár a tagállamok felelőssége a hibrid fenyegetésekre való reagálás, azonban a koordinált uniós fellépéseknek az alábbi keretek mentén szükséges megvalósulni:

- a demokrácia és a nemzetközi jog védelmét kell szolgálniuk;
- az Unió célkitűzéseinek elérését kell szolgálniuk;
- arányosnak kell lenniük az egyes hadjáratokkal;
- helyzetismereten kell alapulniuk;
- figyelembe kell venniük a tágabb összefüggéseket;
- tiszteletben kell tartaniuk a nemzetközi jogot, valamint védeniük kell az alapvető jogokat és szabadságokat.

Érdemes visszatekinteni e Tanács által kiadott következtetésnél az alfejezet elején említett „spill over" hatás kapcsán megfogalmazottakra: a korszellem bármikor kiterjeszthető az Európai Unió normatív szabályzóinak hatáskörét, ami a kiberbiztonság területén számos kapcsolódó terület egységes szabályozását fogja indukálni.

A globális ellátási láncok kitettségét már a Covid19 járvány is hangsúlyossá tette, a háború ezt még inkább felerősítette. Tekintettel az uniós információs és kommunikációs technológiai (IKT) ellátási láncok biztonságára, 2022 októberében a Tanács következtetéseket fogadott el, amelyben az IKT ellátási láncok megerősítését szorgalmazta.[43]

2022 novemberében az Európai Parlament új kiberbiztonságra vonatkozó jogszabályt fogadott el,[44] amelynek célja szigorúbb követelmények támasztása a vállalatokkal, a közigazgatással és az infrastruktúrákkal szemben. A jogszabály megfogalmazza, hogy a tagállamoknak egységes szinten szükséges szabályozni a kibervédelmi képességeiket, intézkedéseiket, ugyanis az eltérőség csökkenti az Európai Unió egységes felkészültségét. Ezzel párhuzamosan az Európai Bizottság előterjesztette

[41] Cyber posture: Council approves conclusions (https://www.consilium.europa.eu/hu/press/press-releases/2022/05/23/cyber-posture-council-approves-conclusions/).

[42] Council conclusions on a Framework for a coordinated EU response to hybrid campaigns (https://www.consilium.europa.eu/hu/press/press-releases/2022/06/21/council-conclusions-on-a-framework-for-a-coordinated-eu-response-to-hybrid-campaigns/).

[43] A Tanács megállapodott az IKT-ellátási láncok biztonságának megerősítéséről (https://www.consilium.europa.eu/hu/press/press-releases/2022/10/17/the-council-agrees-to-strengthen-the-security-of-ict-supply-chains/).

[44] Európa kiberbiztonságának megerősítése: új jogszabályt fogadott el az EP | Hírek | Európai Parlament (https://www.europarl.europa.eu/news/hu/press-room/20221107IPR49608/europa-kiberbiztonsaganak-megerositese-uj-jogszabalyt-fogadott-el-az-ep).

az uniós kibervédelmi politikáról szóló közös közleményt és a katonai mobilitásról szóló cselekvési terv új verzióját,[45] amelyek célja az Ukrajna elleni orosz agresszió következtében egyre romló biztonsági környezet kezelése, valamint a polgárok és az infrastruktúra védelmét célzó uniós képességek javítása. A koncepció négy pillérre támaszkodik:

- együttes fellépést szorgalmaz az erősebb kibervédelmi képességek kialakítására vonatkozóan;
- garantálni szükséges az uniós védelmi ökoszisztéma biztonságát;
- a kibervédelmi képességekbe való beruházás, illetve

a közös kihívások kezelésében való szorosabb együttműködés.

[45] Kibervédelem: az EU erőteljesebben lép fel a kiberfenyegetésekkel szemben, Text, European Commission – European Commission (https://ec.europa.eu/commission/presscorner/detail/hu/ip_22_6642).

KASSAI KÁROLY

A kibertérműveleti képesség szerepének, jelentőségének és fókuszának evolúciója a NATO stratégiai dokumentumai alapján

A kibertér napi életünkben számtalan formában megjelenő, esetenként pontosan nem megfogalmazott közeg, melynek sajátosságaira az elmúlt években egyre több figyelem irányul.

A nemzetközi történések politikai, gazdasági, műszaki, jogi, rendvédelmi, nemzetbiztonsági, katonai és egyéb szempontból egyaránt rávilágítanak, hogy a korábban csak műszaki vagy informatikai „dolog"-nak (vagy számítástechnikai területű kérdésnek) tekintett kibertér – mint környezet – sokszínű lehetőségeket, illetve ezzel párhuzamosan számtalan fenyegetést hordoz magában.

Hazánkban lassan publikációkban is követhető a katonai műveleti alkalmazásra vonatkozó igények megjelenése, ugyanakkor a kérdés átfogó vizsgálata még várat magára, akárcsak a komplexebb védelmi-biztonsági szisztémában való részletező elhelyezés.A helyzetet nehezíti, hogy a katonai kiberműveleti képességeket az általános szintnek megfelelő említéseknél részletesebb, konkrét információkat feltáró publikációk száma erősen korlátos. Vélhető, hogy a nemzeti képességekre vonatkozó adatok, működési paraméterek inkább minősített adatkörbe tartoznak.

Ugyanígy problémás lehet a kiberműveletek kérdésének megközelítése a nemzeti felelősség oldaláról, ahol az esetek nagy részében a békeállapotú, a válsághelyzeti és háborús feladatok elkülönítése nem minden esetben érzékelhető, illetve az ezen helyzetekre vonatkozó nemzeti követelmények is erősen eltérnek.[1]

A katonai erő alkalmazása katonai nemzetbiztonsági (és egyéb nemzetbiztonsági) támogatás nélkül megvalósíthatatlan, így ezzel a kiegészítéssel, komplexen célszerű kezelni és vizsgálni ezt az összetett feladatrendszert.

A magyar képességek kialakítása és fejlesztése napjainkban önállóan nem értelmezhető folyamat, figyelemmel NATO- és EU-tagságunkra és az ebből következő együttműködési kötelezettségre. Ezt fókuszban tartva jelen publikáció nem a kérdés magyar megoldását célozza, hanem annak megalapozása érdekében a NATO stratégiai szintű folyamatok áttekintését vállalja a helyzet tisztázása érdekében. Terjedelmi okok miatt a vizsgálat elsődleges források tükrözésére korlátozódik. Másodlagos

[1] A nemzetközi kommunikáció során kiemelt figyelmet kell fordítani e sajátosságokra, különben nagyon könnyen téves kép alakulhat ki egy-egy megjegyzés, lábjegyzet figyelmen kívül hagyása miatt (pl. „csak háborús helyzetben", „csak nemzeti alkalmazásra", „külön kormányzati felhatalmazás alapján").

források felbukkanása már érzékelhető, de e kör feldolgozása következő lépésként képzelhető el az egymásra épülés logikája szerint, lényegesen szélesebb erőforrások bevonásával.

Az említett, elsődleges forrásfeldolgozás magyar szempontból nem tekinthető teljesen kihasználtnak, de két példa említést érdemel. Szentgáli Gergely 2013-as munkájában áttekintette és jól követhetően összegzi az 1999–2013-as időszak NATO stratégiai szintű történéseit. Javaslatai (naprakészen frissített tudás és rendszer, offenzív képesség és elrettentés, együttműködés, kibervédelmi gyakorlatok, stratégiai szintű gondolkodás) a mai napig helytállónak tekinthetők.[2]

Fekete-Karydis Klára – Lázár Bence 2020-as cikkükben átfogóan bemutatták a NATO kibervédelem szempontjából legfontosabb védelempolitikai szintű eseményeit. A beszámoló értéke a NATO szakmai koncepció és politika lényegi ismertetése, illetve a kiber szakterület szempontjából lényeges szakmai szervezetek és testületek bemutatása.[3]

Adminisztratív megjegyzés, hogy az adatgyűjtés és adatfeldolgozás tudatosan csak nyílt adatokra korlátozódik, így a bizalmasság magasabb szintjét elérő adatok, következtetések e munka eredményeképpen nem lesznek elérhetők.

1. A KATONAI ALKALMAZÁS SZÜKSÉGESSÉGE A KIBERTÉRBEN – AZ 1999-ES NATO STRATÉGIAI KONCEPCIÓ ÉRVÉNYESSÉGE IDEJÉN

A publikációk gyakran idézik a *2016-os varsói NATO-csúcsértekezlet döntését*, mely szerint a kibertér a szárazföldi, tengeri vagy légi területekhez hasonlóan műveleti területként kezelendő,[4] így a köztudatban ez az esemény könnyen azonosítható a kibertér katonai alkalmazására vonatkozó stratégiai döntések eredőjeként.

E kiindulási pont mellett megemlítendő egy évtizeddel korábbról származó nemzeti forrás. Az amerikai *2004-es Nemzeti Katonai Stratégia* megfogalmazta, hogy a fegyveres erőknek rendelkezni kell képességekkel a levegőben, szárazföldön, tengeren, világűrben vagy a kibertérben – a harctér műveleti területein – műveleti képességekkel.[5] Ez konkrét feladatszabás a *2006-os Nemzeti Katonai Kibertér Műveleti Stratégia* számára, ami bevezetésként megállapítja, hogy a Védelmi Minisztérium

[2] Szentgáli Gergely: The NATO Policy on Cyber Defence: The Road so Far. *AARMS*, 2013/1. szám, 83–91 o.

[3] Fekete-Karydis Klára – Lázár Bence: A kibervédelem katonai dimenziói. *Hadtudományi Szemle*, 2020/3. szám, 44–48. o.

[4] Pontos fogalmazás szerint: „(we)… recognise cyberspace as a domain of operations". 2016 Warsaw Summit Communiqué, 70. E mellett megjegyzendő, hogy a kibertér nem „hadműveleti terület/domain", nem „ötödik domain", illetve nem „ötödik haderőnem".

[5] The Military Strategy of United States of America (A Strategy for Today; A Vision for Tomorrow), 2004; 18. o.

függ a kibertértől a nemzeti katonai célok megvalósítása során katonai, hírszerző és adminisztratív (business) területeken.

A minisztériumnak teljes körű katonai műveleteket kell végrehajtani a kibertérben vagy azon keresztül az amerikai érdekek elleni fenyegetések legyőzése (defeat), az eltántorítás (dissuade) és elrettentés (deter) érdekében. A minisztérium hálózatfelderítést (exploitation) fog végezni a hírszerzési adatok beszerzése érdekében és a szükséges mértékben alakítani fogja a kiberteret integrált offenzív és defenzív műveletek formájában.

A kibertérben vagy azon keresztül végzett műveletek a kívánt hatások elérése érdekében megkövetelik a szervezetek, képességek, funkciók, technológiák és műveletek integrálását. A követelményeknek összhangban kell lenniük a jogi és politikákban megfogalmazott követelményekkel, kommunikálni kell a partnerekkel.

A tervezés korai összehangolása segít megoldani a szervezetek együttműködési gondjait, csökkenti az erőforrások hiányosságaiból adódó problémákat, így növeli a kibertérműveletek sikerét.

A törvényes célmeghatározást (targeting) biztosító eljárások integrálása kulcsfontosságú eleme a kibertérműveletek tervezésének.[6]

Gyakorlati szempontból a NATO kiberfenyegetésekre történő első nagyobb szervezeti reagálása 1999. április elején a délszláv válsághoz köthető, amikor NATO-honlapokat, illetve nyílt levelező szolgáltatásokat értek szerb támadások.[7]

A *NATO 1999-es Stratégiai Koncepció*ja az akkori biztonsági helyzetben (hidegháború utáni változások) a kibertér katonai felhasználhatóságával még nem foglalkozik, de a biztonsági kihívásokra történő reagálások között az információs veszélyek már megjelennek.

A dokumentum fenyegetések területén megállapítja, hogy állami és nem állami ellenfelek megpróbálhatják kihasználni a Szövetség növekvő függőségét az információs rendszerektől, az ilyen rendszerek megzavarására tervezett információs műveletekkel. Ezek a szereplők megpróbálhatnak ilyen stratégiákat alkalmazni a NATO hagyományos fegyverek területén lévő fölénye ellen.

A megfelelő katonai képesség fenntartása, a felkészültség, a közös védelem érdekében történő fellépés továbbra is központi szerepet játszik a szövetség biztonsági céljai között.[8]

Abban az időszakban a délszláv válság nehezítette az amúgy is bonyolult 1999-es NATO csatlakozási folyamatot. A szövetségi követelmények szerint[9] jogszabályok-

[6] National Military Strategy for Cyberspace Operations; 2006; előszó, 2, 10. o.

[7] Serbs launch cyberattack on NATO, 1999.

[8] The Alliance's Strategic Concept (1999) Approved by the Heads of State and Government participating in the meeting of the North Atlantic Council in Washington D.C; 23, 28. o.

[9] C-M (55) 15 (FINAL) Security within the North Atlantic Treaty Organization (hatályon kívül). Az akkor érvényben lévő törvény fordítása szerint „Biztonsági Szabályzat" – a NATO szóhasználat a dokumentumot egyszerűsítve „Security Policy"-nak nevezi.

kal megalapozottan azonosítani kellett a NATO minősített adatok biztonságáért felelős nemzeti szervezetet (Nemzeti Biztonsági Felügyelet),[10] ki kellett alakítani a NATO rejtjelanyagok és a NATO minősített adatok centralizált cseréjét és felügyeletét biztosító szervezeteket a Nemzeti Rejtjelelosztó Központ (National Disrtibution Authority)[11] és a Központi Nyilvántartó (Central Registry)[12] formájában.

Látható, hogy a NATO minősített adatok védelmére vonatkozó követelmények önálló jogszabályokban jelentek meg, párhuzamosan a nemzeti minősített adatok védelmére vonatkozó szabályokkal.[13]

Kiemelt fontosságú technikai és biztonsági feladatként meg kellett teremteni a NATO-val történő minősített elektronikus adatkapcsolathoz szükséges feltételeket.[14]

Az említett központi feladatok mellett az egész országra kiterjedően ki kellett alakítani a NATO minősített adatcserét biztosító szolgáltatásokat is, ami nem csak katonai feladat, így az érintett egyéb minisztériumok számára is feladatok jelentek meg. A későbbi években intenzíven kezdtek megjelenni a NATO beruházási programok, ami jelzi, hogy az azokban részt vevő (illetve pályázó) cégeknek is teljesíteni kellett a NATO minősített adatkezelésre vonatkozó összes követelményét.

Ez mutatja, hogy a kétezres évek első fele a NATO információvédelmi követelményeinek megismerésével és egyre kiterjedtebb alkalmazásával telt. Az időszakra vonatkozóan részletesebb szakmai publikációk nem születtek. A NATO-követelmények ismertetése egy kiadványban történt,[15] az időszakra vonatkozó elektronikus információbiztonsági szakmai érdekességek – a NATO-val kapcsolatos specialitásokkal együtt – egy korábbi cikkben olvashatók.[16]

[10] A Nemzeti Biztonsági Felügyeletről szóló 1998. évi LXXXV. törvény (hatályon kívül).

[11] A rejtjelzésre is vonatkozó, az elektronikus információvédelemről szóló 33/2022. (HK. 13.) HM utasítás a nemzeti és a NATO követelmények együttes végrehajtását célozta, de megfogalmazása csak a Központi Rejtjelfelügyeletre terjed ki, a Nemzeti Rejtjelelosztó Központot nem említi annak ellenére, hogy ez a szervezet is a szakmai struktúra része volt.

[12] 4/2000. (II. 29.) HM rendelet a Központi Nyilvántartó, a nyilvántartó és az ellenőrző pont működési rendjéről (hatályon kívül). A részletes feladatokat a Magyar Köztársaság NATO-NYEU Központi Nyilvántartó, Ellenőrző pontok és a biztonsági megbízottak által vezetendő okmányokról szóló 13/2000. (HK. 6.) HM utasítás (hatályon kívül) szabályozta.

[13] A nemzeti feladatokat az állam és szolgálati titokról szóló 1995. évi LXV. törvény szabályozta. E törvény módosításával jelent meg a nemzetközi szerződés alapján átvett, vagy nemzetközi kötelezettségvállalás alapján készült minősített, valamint korlátozottan megismerhető adat védelmének eljárási szabályairól szóló 56/1999. (IV. 2.) Korm. rendelet (hatályon kívül), melynek feladata kifejezetten a NATO-követelmények megvalósítása.

[14] 82/2002. (HK. 26.) HM utasítás a NATO Irodaautomatizálási rendszer (NIAR) biztonságával kapcsolatos feladatokról.

[15] *Biztonság és Titokvédelem a NATO szabályai szerint.* Budapest, Honvéd Kiadó, 1999, 1. o.

[16] Kassai Károly: Az elektronikus információvédelem felső szintű szervezeti és szakmai történései a 2005–2015 közötti időszakban. *Hadmérnök*, 2015/3. szám 279–291. o.

Az említett törekvések egyértelműen csak a minősített adatkezelés védelmét célozták, a nyílt (nem minősített) adatkezelés jogszabályi követelményei még nem álltak rendelkezésre.[17] Így ebben az időszakban hivatalos kibervédelmi (vagy kibertérműveleti) nemzeti megfogalmazások nyilvánosan nem azonosíthatók.

A *NATO 2002-es prágai csúcsértekezletén* megfogalmazott Prágai Képesség Kötelezettség Vállalás (Prague Capabilities Commitment – PCC) jóváhagyása – mint a szövetség folyamatos erőfeszítéseinek része – egyértelmű válasz az érzékelt fenyegetésekre. A Vállalás célja a magas fenyegetettségű környezetben új katonai képességek erősítése és fejlesztése a modern hadviselés érdekében. Itt már megjelenik a kibertér biztonsága, mert a deklaráció szerint *meg kell erősíteni a kibertámadások elleni védelmi képességeket.*[18]

A 2002-es év az új Biztonsági Politika megjelenésével a NATO minősített adatok védelmére vonatkozóan fontos mérföldkő.[19] Az addigi szabályozási struktúra megőrzésével a politika rögzíti a minősített adatok védelmére vonatkozó stratégiai követelményeket, illetve a fizikai, személyi, adminisztratív, elektronikus információvédelmi és iparbiztonsági követelményeket a NATO-szervezetek és -tagállamok részére.

A következő szabályozási szinten a szakterületeket szabályozó direktívák (kötelező szabályok és eljárások), ajánlások és támogató dokumentumok találhatók. Ebben a rendben már azonosíthatók olyan elektronikus információvédelmi szakfeladatok (pl. kockázatelemzés, detektálás, eseménykezelés, biztonsági audit, helyreállítás) ami napjainkban a kibervédelmi szakfeladatokkal is kapcsolatba hozhatók.

A további, felső szintű NATO védelempolitikai dokumentumok egyre összetettebben említik a kibertérben érzékelhető fenyegetéseket és a szükséges képességfejlesztést. A *2004-es isztambuli csúcsértekezlet* kivételnek tekinthető, mert szorosan kapcsolódó követelményeket, megállapításokat nem fogalmaz meg.[20]

A *2006-os rigai csúcsértekezlet* a kapacitások fejlesztése céljaként említi a szövetség műveleteiben *az adatok, hírszerzési információk megbízható, biztonságos és késedelem nélküli megosztását, közben javítva a kulcsfontosságú információs rendszerek kibertámadások elleni védelmét.*[21]

[17] A NATO minősített adatok védelmére vonatkozó szabályok egy része tartalmazott nyílt (nem minősített) adatok védelmére vonatkozó követelményeket is.

[18] Prague Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Prague, Czech Republic, 2002, 4. c, f. p. Ez alapján kezdődött meg a NATO Eseménykezelő Központ (NATO Computer Incident Response Capability – NCIRC) kialakítása.

[19] C-M (2002) 49 Security within the North Atlantic Treaty Organization.

[20] Istanbul Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council, 2004.

[21] Riga Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Riga on 29 November 2006; 24. o.

A *2006-os (a rigai csúcsértekezleten elfogadott) NATO Átfogó Politikai Irányelv* megállapítja, hogy a NATO elleni jövőbeli támadások az aszimmetrikus eszközök használatának fokozott kockázatával járnak.

A NATO-nak meg kell őriznie képességét a missziók teljes körének lebonyolítására, a magas intenzitásútól az alacsonyig, különös figyelmet fordítva a legvalószínűbb műveletekre, reagálva a jelenlegi és jövőbeli hadműveleti követelményekre.

Tekintettel a jövőbeli biztonsági környezet jellegére, annak hatásaira, a szövetségnek mozgékonyságra és rugalmasságra van szüksége az összetett és kiszámíthatatlan kihívások megválaszolásához, amelyek a tagállamok határaitól távol alakulhatnak ki, és rövid időn belül mutatkoznak meg.

Az Irányelv a következő 10-15 évre a fejlődő biztonsági környezet, valamint a hagyományos és különösen az aszimmetrikus fenyegetések, kockázatok kezelése érdekében azonosítja a szükséges képességkövetelményeket. Ebben szerepel a létfontosságú infrastruktúrák és katonai erők védelme, a szövetség számára kritikus fontosságú információs rendszerek kibertámadások elleni védelme, illetve a műveletek vezetéséhez szükséges képességek (figyelemmel a tapasztalható fenyegetésekre).[22]

2006-os nemzeti esemény, hogy a Puskás Tivadar Közalapítvány keretein belül működő Kormányzati Hálózatbiztonsági Központ nemzetközi minősítést ért el, amivel teljes körű tagjává vált az európai CERT[23]- közösségnek. Ez kezdeti lépés, hogy megkezdődhessen a nemzeti szinten értelmezhető eseménykezelés, illetve a nemzetközi eseménykezelőkkel történő együttműködéssel riasztási, értesítési információkat kaphassanak az érintettek, illetve szakértői szintű konzultációk támogassák egy-egy technikai ügy megoldását.

A *NATO 2008-as bukaresti csúcsértekezlete* megállapítja, hogy a NATO továbbra is elkötelezett a szövetség kulcsfontosságú információs rendszereinek megerősítésében a kibertámadások ellen. A Kibervédelmi Politikára[24] hivatkozva hangsúlyozza annak szükségességét, hogy a NATO és a nemzetek saját felelősségük szerint védjék meg a kulcsfontosságú információs rendszereket, osszák meg bevált gyakorlataikat, és legyenek képesek felkérésre segítséget nyújtani más szövetséges nemzeteknek kibertámadás esetén.[25]

A 2008-as év eseménye, hogy a 2007-es Észtországot ért elektronikus szolgáltatások elleni súlyos támadások a nemzetközi és a NATO-figyelmet a kibervédelemre irányították. A NATO saját rendszerek védelmére irányuló erőfeszítése mellett a kutatási, képzési feladatok, kibervédelmi gyakorlatok és egyéb jövőbeli képességek

[22] Comprehensive Political Guidance, 2006; 5, 7, 10, 16. c, d, e. p.

[23] Computer Emergency Response Team (CERT), az eseménykezelést, koordinálást végző szakértő szervezet egyik nemzetközi megnevezése. Ebben az esetben „CERT – Hungary" azonosítással az említett szervezet akkreditált taggá vált.

[24] Policy on Cyber Defence.

[25] Bucharest Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest on 3 April 2008; 47. o.

támogatására irányuló tevékenységek érdekében Tallinnban megalakult a NATO Kibervédelmi Kiválósági Központ.[26]

A 2008-as évben indult a NATO Cyber Coalition kibervédelmi gyakorlatsorozat, ami azóta az egyik legnagyobb ilyen típusú rendezvény a világon. A gyakorlatot a NATO Transzformációs Parancsnokság tervezi és irányítja a NATO Katonai Bizottság felügyeletével.

A gyakorlatsorozat a NATO-szervezetek, a szövetségesek és a partnerek kiberkoalícióját képviseli, hogy megerősítse a szövetség képességét a kibertérben és azon keresztüli fenyegetésekkel kapcsolatos elrettentésre, védelemre és a fenyegetések elleni küzdelemre, támogatva a NATO alapvető feladatait az együttműködési és kibertéri műveletek gyakorlásával.[27]

A 2008-as év egyben a Gripen vadászrepülők rendszerbe állítását is jelenti. A stratégiai szintű feladatok mellett – a részletek említése nélkül – érdemes röviden említeni, hogy ebben az esetben a NATO elektronikus információvédelmi keretrendszerének alkalmazására volt szükség a levegő-levegő és föld-levegő, valamint földi kiszolgáló elektronikus információs rendszerek biztonságának szavatolása érdekében.[28]

A *NATO 2009-es Strasbourg–Kehl csúcsértekezletének* deklarálása szerint a szövetség továbbra is elkötelezett a kommunikációs és információs rendszerek kibertámadások elleni megerősítése mellett, amelyek kritikus fontosságúak a NATO számára.[29] A támadások megelőzése, az azokra adandó válaszreagálások érdekében – összhangban a Kibervédelmi Politikával – Kibervédelmi Menedzsment Felügyelet[30] alakult a meglévő Számítógépes Incidenskezelő Képesség[31] hatékonyságának növelése érdekében, illetve Észtországban megalakult a NATO Kibervédelmi Kiválósági Központ.[32] A fenyegetések ellensúlyozása érdekében a szövetség felgyorsítja kibervédelmi képességek fejlesztését a teljes felkészültség elérését célozva. Emellett a kibervédelem a NATO-gyakorlatok szerves részévé válik.

[26] NATO Cooperative Cyber Defence Center of Excellence (NATO CCD COE). Centre is the first International Military Organization hosted by Estonia, (https://ccdcoe.org/news/2008/centre-is-the-first-international-military-organization-hosted-by-estonia/).

NATO opens new centre of excellence on cyber defence (https://www.nato.int/cps/en/natohq/news_7266.htm).

[27] Cyber Coalition: NATO's Flagship Cyber Exercise (https://www.act.nato.int/cyber-coalition).

[28] Mit tud egy magyar Gripen (https://honvedelem.hu/hirek/mit-tud-egy-magyar-gripen.html).

[29] Állami és nem állami szereplők megpróbálhatják kihasználni a szövetség és szövetségeseinek egyre növekvő függőségét e rendszerektől.

[30] Cyber Defence Management Authority.

[31] Computer Incident Response Capability – CIRC.

[32] NATO Cooperative Cyber Defence Centre of Excellence – NATO CCD COE.

A szövetség tovább erősíti a kapcsolatokat a NATO és a partnerországok között a kibertámadások elleni védelem terén.[33]

A 2009-es évhez tartozó nemzeti esemény a minősített adatok védelme szempontjából sorsfordulatot jelentő törvény,[34] valamint az ezt követően megjelenő végrehajtási rendeletek, melyek egyértelmű megfogalmazással már együttesen kezelték a NATO, EU (és egyéb külföldi) valamint nemzeti minősített adatok védelmét.[35]

Az egységesített szabályok mellett megjegyzendő, hogy ekkor következett be a most is tapasztalható állapot, mely szerint a nemzeti, NATO, EU (vagy egyéb külföldi) minősített adat felügyeletét a korábbi megosztott szerepek helyett[36] egy szervezet – a Nemzeti Biztonsági Felügyelet – látja el.

A *NATO 2010-es liszaboni csúcsértekezlete* megállapítja, hogy a kiberfenyegetések száma növekszik, bonyolultságuk erősödik. A folyamatos és szabad kibertér hozzáférésének biztosítása – valamint a kritikus fontosságú rendszerek sértetlenségének biztosítása – érdekében a szövetség doktrinális területen is figyelembe veszi a modern konfliktusok kiberdimenzióját,[37] és fejleszti képességeit a detektálás, vizsgálat, megelőzés, védelem és helyreállítás érdekében a szövetség számára kritikus fontosságú rendszerek elleni kibertámadások esetén.

A szövetség kiemelten törekszik, hogy 2012-re gyorsítsa a NATO Számítógépes Eseménykezelő Képesség teljes készenlétét,[38] és az összes NATO-szervezetet központosított kibervédelem alá vonja.

A NATO védelmi tervezési folyamatot[39] felhasználva történik a szövetségesek kibervédelmi képességeinek fejlesztésének elősegítése, az egyes szövetségesek kérésre történő segítése, valamint az információmegosztás, az együttműködés és az interoperabilitás optimalizálása.

[33] Strasbourg / Kehl Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Strasbourg / Kehl, 2009; 49. o.

[34] Mavtv.

[35] Ez a szabályozási környezet nem vonatkozik a nyílt (nem minősített) adatok védelmére.

[36] Korábban a nemzeti titokvédelemért a Belügyminisztérium, a rejtjelzés felügyeletéért az Országos Rejtjelfelügyelet, illetve a NATO, EU minősített adatok védelmének felügyeletéért a Nemzeti Biztonsági Felügyelet volt felelős.

[37] A megállapítás a NATO Összhaderőnemi Doktrína (AJP 01) első olyan módosítására utal 2010-ben, amelyben megtörtént a kibertér szempontjainak figyelembevétele. Ez kritikus fontosságú szabályozási kérdés, mert rámutat arra, hogy összetett szabályozási környezetben a „fentről lefelé" elvet kell követni. Először meg kell fogalmazni a legmagasabb szintű követelményeket, elvárásokat, melynek eredményeképpen az alacsonyabb szintű szabályozókban ezek a követelmények tovább bonthatók, fejleszthetők a jogi normák és egyéb irányelvek figyelembevételével.

[38] Full Operational Capability – FOC.

[39] NATO Defence Planning Process – NDPP.

A kibertérből fakadó biztonsági kockázatok kezelése érdekében a szövetség szorosan együttműködik más szereplőkkel, például az ENSZ-szel és az EU-val (megállapodásnak megfelelően).[40]

2010-es esemény, hogy a NATO Nemzetközi Törzsön belül megalakult Új Típusú Biztonsági Kihívások Igazgatóság[41] a növekvő, nem hagyományos kockázatok kezelése érdekében. Az új szervezet feladata a terrorizmus, a tömegpusztító fegyverek kereskedelme, a kibervédelem és az energiabiztonság kérdéseinek kezelése. Feladata lesz továbbá stratégiai szintű elemző képesség biztosítása, illetve a nemzetközi folyamatok követése, a fejlesztési folyamatokban való részvétel a NATO biztonságára hatással bíró esetekben.[42]

A 2010-es év eseménye, hogy a NATO Kibervédelmi Kiválósági Központ csatlakozott a NATO Cyber Colalition kibervédelmi gyakorlat tervezési, szervezési és végrehajtási folyamataihoz.[43]

2010-ben zajlott a NATO Kibervédelmi Kiválósági Központ rendezésében az első Locked Shields kibervédelmi gyakorlat. Az azóta is folyamatosan fejlődő, bővülő gyakorlat kezdetben erősen technikai szempontú volt, célként kitűzve egy adott infrastruktúra üzemeltetését egyre erősödő támadó körülmények között. Ez a védelmi-támadó tevékenység[44] virtuálisan kialakított különböző infrastruktúrák túléléséért történik, stratégiai döntéshozatallal, jogi kérdések megoldásával, illetve kommunikációs kérdésekkel kiegészítve.[45]

A 2010-es év magyar vonatkozása az első Magyar–NATO Kibervédelmi Együttműködési Megállapodás[46] megkötése a fentiekben említett szövetségi–nemzeti kapcsolattartás erősítése érdekében. A nemzeti kapcsolattartói feladatokat a Miniszterelnökség irányítása alatt álló kormányzati szervezet látta el.

Az évben megtörtént a magyar csatlakozás a NATO Kibervédelmi Kiválósági Központhoz. A feladat új kihívásokat jelentett a központ akkori nemzetközi közösségének, mert a megalakulás óta eltelt két évben még nem volt példa új nemzet csat-

[40] Lisbon Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Lisbon, 2010, 40. o.

[41] Emerging Security Challenges Division (ESCD).

[42] New NATO division to deal with Emerging Security Challenges (https://www.nato.int/cps/en/natohq/news_65107.htm).

[43] Centre Supports NATO's Cyber Coalition 2010 (https://ccdcoe.org/news/2010/centre-supports-natos-cyber-coalition-2010/).

[44] Szakmai megfogalmazás szerint „Blue Team – Red Team".

[45] A NATO Kiválósági Központ nem NATO-szervezet, így ez a gyakorlat sem szövetségi gyakorlat, de említést érdemel, mint egyértelmű gyakorlási lehetőség a központ támogató nemzetei, valamint a NATO-szervezetek és napjainkban már az EU számára is. Locked Shields (https://ccdcoe.org/exercises/locked-shields/).

[46] Memorandum of Understanding – MoU.

lakozási kérelmének befogadására.[47] A csatlakozással megnyílt a lehetőség a központ által szervezett tanfolyamok látogatására, a kibervédelmi gyakorlatokon való részvételre, ami azonnali nemzeti hasznosítást is jelent.

1.1. Az időszak összefoglalása

Az 1999-es NATO Stratégiai Koncepció érvényességének időszakában megkezdődött a szövetség összetett folyamataiban és szervezeti rendjében a kibertér-fenyegetések súlyosságnak megfelelően történő kezelése. Ennek jól érzékelhető mozzanata a NATO-rendszerek védelmi szintjének emelésére irányuló törekvés és a működést biztosító, egész világot behálózó rendszerek központosított eseménykezelési rendjének kialakítása.

A 2001-es amerikai 9/11-es, súlyos terrorcselekmény az általános nemzeti és nemzetbiztonsági fenyegetettségre irányította a figyelmet, míg a 2007-es észt kibertámadások miatt a kiberbiztonság került fókuszba. Ekkor szakmai koncepció, majd politika született a szövetség szintű követelmények, irányelvek rögzítése érdekében. Ezzel megjelent az első felelősséget tisztázó megfogalmazás, mely szerint a NATO elsődleges feladata a saját rendszerek védelme és a szövetségesek évről évre szélesebb körű támogatása, míg a szövetségesek felelősek a nemzeti szintű kibervédelemért.

A NATO-rendszerek védelme, az eseménykezelés biztosítása mellett jelentkező szükségletek alapján újabb szervezeti elemek alakultak a nemzetekkel történő folyamatos technikai szint feletti kapcsolattartás biztosítása, illetve az új típusú fenyegetések kezelése érdekében.

A kibervédelmi kérdések technikai kezelési szükségleteinek felismerésem mellett kiemelt fontosságú e szakterületen is a hírszerzési képesség (lehetőségek) alkalmazásának fontossága.

Az elméleti jellegű kérdések kutatása, az oktatás és képzés támogatása érdekében szakterület szerinti kiválósági központ alakult, illetve a NATO kialakította a kibervédelmi gyakorlatok rendjét.

A NATO–nemzeti gyakorlati együttműködés érdekében kirajzolódott egy együttműködési megállapodásokkal kijelölt keretrendszer.

A vizsgálati cél nem tartalmazza a NATO elektronikus információvédelmi kérdések feldolgozását, de szükség van annak kiemelésére, hogy a védelempolitikai, stratégiai szintű kiberbiztonság (később kibertérművelet) egyszerűen nem tekinthető létező fogalomnak az elektronikus információvédelmi feladatrendszer (követelmények) nélkül.

[47] Hungary joins the Centre (https://ccdcoe.org/news/2010/hungary-joins-the-centre/).

A fenti események jogosan nevezhetők az első NATO kibervédelmi lépéseknek, melyhez az eseményekhez köthetően egyértelműen azonosíthatók az első magyar katonai erőfeszítések is.

2. TOVÁBBI LÉPÉSEK AZ ÚJ STRATÉGIAI KONCEPCIÓ NYOMVONALÁN

A *NATO lisszaboni csúcsértekezletén elfogadott Stratégiai Koncepció (2010)* szerint a kibertámadások egyre gyakoribbak, szervezettebbek és költségesebbek az általuk okozott kár tekintetében, melyek sértik a kormányzati adminisztrációt, a vállalkozásokat, a gazdaságot és potenciálisan a közlekedést, az ellátási hálózatokat és egyéb kritikus infrastruktúrákat.

A támadások elérhetik azt a küszöböt, ami fenyegeti az euroatlanti jólétet, biztonságot és stabilitást. A támadások forrásai lehetnek külföldi katonai és hírszerző szolgálatok, szervezett bűnöző csoportok, terroristák és/vagy szélsőséges csoportok.

A szövetség gondoskodni fog arról, hogy a NATO rendelkezzen a fenyegetések elleni elrettentéshez és az ellenük való védelemhez szükséges képességek teljes skálájával. Továbbfejleszti képességeit a kibertámadások megelőzése, észlelése és védelme érdekében, valamint a támadások után szükséges visszaépítéshez, többek között a NATO védelmi tervezési folyamat felhasználásával a nemzeti kibervédelmi képességek fokozására és koordinálására, az összes NATO-szervezet központi kibervédelem alá vonásával, valamint a kibertudatosság, a figyelmeztetések és válaszlépések jobb integrálásával a tagállamokkal együttműködésben.[48]

A *2011-es NATO Politikai Iránymutatás* a stabilizációs és helyreállítási tevékenységeket tartalmazó műveletekre fókuszálva határoz meg általános követelményeket. E tevékenységek általában civil hatóságok, szervezetek feladatai (de a NATO-nak gyakran szerepet kell vállalnia ezekben a feladatokban is), így ez a dokumentum zömében e speciálisnak tekinthető műveletre, főleg a civil–katonai együttműködésre koncentrál. Lényegi – más esetben is értelmezhető – eleme, hogy egy művelet előtti elkötelezettség előtt a NATO-nak átfogó elemzést és értékelést kell végeznie a lehetséges műveleti területen a politikai, társadalmi-gazdasági és intézményi helyzetről, valamint a fizikai infrastruktúráról.[49]

2011-es esemény, hogy jogszabály jelent meg a válságkezeléshez szükséges Nemzeti Intézkedési Rendszer kialakításáról, összhangban a NATO Válságreagálási

[48] Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization 2010, 12, 19. o.

[49] Political Guidance on ways to improve NATO's involvement in Stabilisation and Reconstruction, 2011, 6. o.

Rendszerrel.[50] A feladatrendszer a napi élet során felmerülő, normál üzemű működéstől eltérő, egyedi intézkedések kezelésének lehetőségét biztosítja. A meghatározott Nemzeti Intézkedések Gyűjteménye (NIGY) a NATO hasonló intézkedéseivel szinkronizált, ami biztosítja a két válságkezelési rendszerben az azonos értelmezést, intézkedések bevezetését.[51]

Az év eseménye az első magyar részvétel a NATO Cyber Coalition kibervédelmi gyakorlatsorozat éves rendezvényén. A nemzetek számára 2010-ben megnyitott kibervédelmi gyakorlaton a magyar szereplőket a Nemzeti Biztonsági Felügyelet koordinálta.[52]

További nemzeti esemény a kibertérműveleti képességek kialakítására vonatkozó koncepció kialakításának elrendelése, ami egyben a NATO képességfejlesztéssel történő összehangolási lépése is.

A szövetségesek előtt álló feladat, hogy nemzeti fejlesztéseiket hangolják össze a NATO-képességfejlesztéssel.[53] Az erre vonatkozó honvédelmi ágazati szintű koncepció kidolgozásának elrendelése miniszteri utasítás formájában történt meg.[54]

A *NATO 2012-es chicagói csúcsértekezlete* deklarációja az idézett, korábbi dokumentumokkal összhangban folytatólagosan megállapítja, hogy a kibertámadások száma továbbra is jelentősen növekszik, kifinomultságuk és összetettségük fejlődik. Emiatt a szövetségesek megerősítik a lisszaboni csúcstalálkozón tett kibervédelmi vállalásukat.

A NATO meglévő képességeire építve a NATO Számítógépes Incidenskezelő Képesség kritikus elemei elérték a teljes működési képességet, a legtöbb üzemeltetési helyszín és felhasználói szám elérésével.

A szövetség elkötelezte magát, hogy erőforrásokat biztosítva, a szükséges reformokat végrehajtva valamennyi NATO-szervezet központosított kibervédelem alá kerüljön.

A szövetségesek a kibervédelmi intézkedéseket tovább integrálják a szövetség struktúráiba és eljárásaiba, és mint egyes nemzetek, továbbra is elkötelezettek a nemzeti kibervédelmi képességek azonosítása és megvalósítása mellett, amelyek erősítik a szövetség szintű együttműködést és interoperabilitást, beleértve a NATO védelmi tervezési folyamatait is.

[50] NATO Crisis Response System (NCRS).

[51] 278/2011. (XII. 20.) Korm. rendelet a NATO Válságreagálási Rendszerével összhangban álló Nemzeti Intézkedési Rendszer rendeltetéséről, feladatairól, eljárási rendjéről, a közreműködők kötelezettségeiről.

[52] Sikeres volt a kibervédelmi gyakorlat (https://honvedelem.hu/hirek/honvedelmi-miniszter/sikeres-volt-a-kibervedelmi-gyakorlat.htm).

[53] Ez nem jelent akadályozást semmilyen önálló nemzeti cél kitűzése és megvalósítása területén, mert a nemzeti képességfejlesztések egyértelműen nemzeti hatáskörben kezelendő ügyek.

[54] 81/2011. (VII. 29.) HM utasítás a honvédelmi tárca Kibernetikai Védelmi Koncepció kialakításához szükséges feladatok meghatározásáról, 3. §. 5–6. o.

A szövetség továbbfejleszti a képességeket a kibertámadások megelőzésére, felderítésére, az azok elleni védelemre és az azokból történő helyreállítás érdekében.[55]

A *NATO-főtitkár 2012-es évről szóló jelentése* szerint a NATO a 2011 októberében indított Intézkedési Terv (Action Plan) révén folytatta az új Kibervédelmi Politika végrehajtását.

2012 tavaszán a NATO fontos szerződést kötött, hogy jelentősen fejlessze egyedi kibervédelmi képességét (NCIRC). A projekt befejezésével 2013 őszén valamennyi NATO-hálózat központosított védelem alatt áll, így a NATO-képesség jelentősen bővül a saját hálózatok védelmében a behatolás és támadás minden típusa ellen.

A NATO jobb helyzetbe kerül ahhoz, hogy segítse a szövetségeseket és a partnereket a kibertámadások felderítésében, az azok elleni védelemben és a támadás utáni helyreállítási tevékenységben, valamint kérésre gyorsreagálású csoportok[56] telepítésében.

A kibervédelmi képességek továbbfejlesztése érdekében a NATO létrehozott egy kiberfenyegetettségértékelő szervezeti elemet,[57] ami megtartotta első teljes körű, kibervédelmi forgatókönyvön alapuló válságkezelési gyakorlatát. A másik éves gyakorlat a „Cyber Coalition" volt, ahol a szövetségeseket és partnereket bevonva tesztelés bizonyította az eseménykezelési és a válságkezelési eljárások hatékonyságát.[58]

A *NATO-főtitkár 2013-ról szóló éves jelentés* megállapítja, hogy az év jelentős előrelépést jelent a NATO kibertámadásokkal szembeni védelme érdekében.

A NATO Számítógépes Incidenskezelő Képesség által biztosított központosított védelem bevezetése megtörtént a NATO-szervezeteknél, így az 51 NATO-helyszínen található NATO-hálózatok átfogó (24/7) felügyelet alatt állnak, továbbfejlesztett érzékelőkkel és behatolásérzékelő technológiákkal védettek.

Kiberterületen (mint műveleti területen) a NATO elsődleges szerepe a saját hálózatok védelme. 2013-ban a szövetség kibővítette erőfeszítéseit a kiberfenyegetések kezelésére. A kibervédelem most először került be a NATO védelmi tervezési folyamatába. Ez támogatást nyújt, hogy a szövetségesek rendelkezzenek az alapvető szervezetekkel, képességekkel és interoperabilitással egymás segítése érdekében.

A NATO az évben folytatta a kibervédelmi forgatókönyvek kialakítását a gyakorlatokon, kiképzéseken és oktatások során.[59]

2013-as speciális szakmai eseménynek tekinthető a NATO Kibervédelmi Kiválósági Központ szervezésében egy nemzetközi jogászcsoport többéves együttműködésén és kiterjedt szakértői konzultációján alapuló kutatás lezárása és a „Tallinn

[55] Chicago Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago on 20 May 2012; 49. o.

[56] Rapid Reaction Teams.

[57] Cyber Threat Assessment Cell.

[58] The Secretary General's Annual Report 2012, "Cyber defence" fejezet, 17. o.

[59] The Secretary General's Annual Report 2013, „Cyber defence" fejezet, 18. o.

Manual"[60] kiadása. A gyűjtemény kiadása frappáns válasz a nemzetközi jog alkalmazhatóságára a kibertéri események megoldása érdekében. A sokat hangoztatott érv, mely szerint nincs kialakult nemzetközi jogi norma a kibertérre, így az ott elkövetett ügyeket nem lehet megítélni, ezáltal más megvilágítást kap. A gyűjtemény a háborús cselekmények megítélésében ad segítséget. A rengeteg forgatókönyvet bemutató munka nem NATO-szabálykönyv, kézikönyv (szabályokkal) vagy jogszabály, hanem a szerzők szakmai véleményét tartalmazó, a szabályok alkalmazhatóságára vonatkozó példagyűjtemény, melynek tanulmányozása, az analógiák felismerése segíthet egy-egy kibertéri történés jogi megítélésében.[61]

2013-ban belga kezdeményezéssel indult nemzetközi útjára a Károskód Információcsere Platform,[62] melynek célja a rosszindulatú kódok jellemzőivel kapcsolatos információk megosztása egy megbízható közösségen belül a támadás részleteinek megosztása nélkül. A platform már működik néhány nemzet és a NATO Számítógépes Incidenskezelő Képesség között. A projekt végső célja egy olyan NATO-képesség kialakítása, ami minden NATO-nemzet számára elérhető, és amire a nemzetek rábízzák az információk megosztását.[63]

2013-as nemzeti esemény, hogy kormányhatározat döntött a kormányzati hálózatbiztonsági feladatokat ellátó Puskás Tivadar Közalapítvány megszüntetéséről. Ennek megfelelően a kormányzati feladatok a Nemzetbiztonsági Szakszolgálathoz kerültek, figyelemmel a kiadás előtt álló, elektronikus információbiztonsági törvényre.[64]

A határozat egyben emlékeztet, hogy hazánkban 2005-ben kezdődött hivatalosan a kormányzati eseménykezelés, információcserét, konzultációt biztosítva az igénylő szervezetek részre. Honvédelmi szempontból ez még nem jelentett napi jellegű technikai információcserét, de részletek említése nélkül is kijelenthető, hogy az eseti jellegű együttműködés hatékony segítség volt a felek számára.

Az évben később megjelenő elektronikus információbiztonságról szóló törvény[65] több szempontból is kritikus eleme a magyar elektronikus információbiztonságnak. Ezt megelőzően az elektronikus információs rendszerek biztonságára vonatkozóan nem állt rendelkezésre egyértelmű, jogszabályokban meghatározott követelmény.

Az új jogszabályok (a törvény és végrehajtási rendeletei) meghatározzák az alapvető feladatokat, kijelölik a nemzeti szintű felelős szervezeteket (eseménykezelés és

[60] Tallinn Manual on the International Law Applicable to Cyber Warfare.

[61] Peacetime Regime (https://ccdcoe.org/news/2013/newsletter-peacetime-regime/).

[62] Malware Information Sharing Platform (MISP).

[63] Sharing malware information to defeat cyber attacks, (https://www.nato.int/cps/en/natohq/news_105485.htm).

[64] 1284/2013. (V. 27.) Korm. határozat a Puskás Tivadar Közalapítvány megszüntetésével kapcsolatos feladatokról.

[65] 2013. évi L. törvény az állami és önkormányzati szervezetek elektronikus információbiztonságáról.

elektronikus biztonsági hatóság), és meghatározzák például az események bejelentésére vonatkozó kötelezettséget, ami egyértelműen segíti a honvédelmi és a nemzeti szintű együttműködést.[66]

2013-ban a vonatkozó jogszabályi követelmények szerinti ágazati szinten meg kellett határozni az elektronikus információs rendszerek biztonságával kapcsolatos felelősségeket, hatásköröket. Ennek megfelelően megtörtént a honvédelmi ágazati kijelölés, miniszteri rendelet formájában.[67]

A *NATO 2014-es walesi csúcsértekezlete* további lényeges tartalmi elemeket határoz meg. A fenyegetések kapcsán a dokumentum megállapítja, hogy a kibertámadások elérhetik azt a küszöböt, ami veszélyezteti a nemzeti és euroatlanti jólétet, biztonságot és stabilitást. Hatásuk ugyanolyan káros lehet a modern társadalmakra, mint egy hagyományos támadás. Ezért a szövetség megerősíti, hogy a kibervédelem a NATO alapvető feladatának, a kollektív védelemnek a része.

A szövetségesek elkötelezettek a nemzeti kibervédelmi képességek továbbfejlesztésében, és erősíteni fogják azon nemzeti rendszerek kiberbiztonságát, melyektől a NATO alaprendeltetésű feladatai függenek, a szövetség ellenálló képessége és teljes mértékű védelme érdekében.

A szoros kétoldalú és multinacionális együttműködés kulcsfontosságú szerepet játszik a szövetség kibervédelmi képességeinek fejlesztésében.

A szövetségesek folytatják a kibervédelem NATO-műveletekbe, hadműveletekbe és a folytonossági (contingency) tervekbe történő integrálását, és erősítik az információcserét és a helyzetismeretképet (situation awareness) a szövetségesek között.[68]

2014-es esemény, hogy a nemzeti felkészülés érdekében megjelent a NATO elektronikus információbiztonsági és kiberbiztonsági[69] minimum követelményrendszer azon nemzeti információs infrastruktúrák számára, melyek kritikusan fontosak a szövetség alaprendeltetésének biztosításához.

A *NATO-főtitkár 2014-es évre vonatkozó jelentése* szerint előretekintve látható, hogy a számítógépes fenyegetések és támadások egyre gyakoribbak, kifinomultabbak és potenciálisan károsak.

[66] A törvény a bevezetőben megfogalmazza, hogy a kiberbiztonság a bizalmasság, sértetlenség és a rendelkezésre állás megvalósulásával biztosítható. Ezzel együtt a törvény az elektronikus információbiztonságról szól, így túlzásnak tekinthető azt „kibertörvény"-ként említeni.

[67] Szakmai érdekesség, hogy a NATO-csatlakozás idejében szükséges jogi szabályozáson kívül miniszteri rendelet ezen a szakterületen nem jelent meg. 16/2013. (VIII. 30.) HM rendelet a Magyar Honvédség, a Katonai Nemzetbiztonsági Szolgálat, a Honvédelmi Tanács és a Kormány speciális működését támogató elektronikus infokommunikációs rendszerek biztonságának felügyeletéről és ellenőrzéséről (hatályon kívül).

[68] Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, 2014, 72–73.

[69] Pontos kifejezés szerint: CIS Security (including cyber defence).

A kiber domain változó kihívásaira reagálva a NATO vezetői a szeptemberi walesi csúcstalálkozón jóváhagyták a NATO Megerősített Kibervédelmi Politikát és az Intézkedési Tervet. A politika megállapítja, hogy a kibervédelem a szövetség kollektív védelem alapfeladatának része, megerősíti, hogy a nemzetközi jog érvényes a kibertérben, illetve fokozni kell a NATO és az ipar közötti együttműködést.

A NATO kibervédelem legfontosabb prioritása a NATO tulajdonában lévő és üzemeltetett kommunikációs rendszerek védelme.

2014 májusában a NATO Számítógépes Incidenskezelő Képesség elérte a teljes működési képességet, és a NATO-hálózatok védelmét 52 helyszínre bővítette.

A NATO 2014-ben is folytatta a kibervédelmi komponensek beépítését gyakorlatokba, képzésekbe és az oktatásba.

2014 novemberében a szövetség megtartotta eddigi legnagyobb kibergyakorlatot a NATO Cyber Range (tesztlabor) segítségével, ami egy szoftveralapú megoldások tesztelésére és értékelésére szolgáló platform a biztonsági problémák megoldása érdekében.[70]

A *NATO-főtitkár 2015-ös évre vonatkozó jelentése szerint a* NATO folyamatosan figyelemmel kíséri a kiber domainben tapasztalható fenyegetések gyors evolúcióját – nemcsak mennyiség, hanem a bonyolultság tekintetében is.

Növekvő jelleggel tapasztalható a kártékony szereplők előnyszerzése a digitális alvilágban, mint a gyors és költséghatékony megoldás a céljaik elérése (szolgáltatásmegszakítás vagy sérülések okozása).

A szövetség az első Kibervédelmi Politikát 2008-ban adta ki, röviddel az Észtországot érő súlyos kibertámadások után. A NATO 2014-ben elfogadta az új Megerősített Kibervédelmi Politikát és az Intézkedési Tervet.

A politika megfogalmazza, hogy a kollektív védelem részeként a kibervédelem a NATO alaprendeltetésű feladata (core task), megerősíti, hogy a nemzetközi jogot alkalmazni kell a kibertérben, és fokozni kell a NATO együttműködését az ipari szektorral.

Az elsődleges feladat (top priority) a szövetség tulajdonában vagy üzemeltetésében lévő CIS-védelem.

A NATO a kibervédelmet integrálta a védelmi tervezési folyamatba, a műveleti tervezésbe, a válságkezelési rendszabályokba, valamint a katonai és politikai jellegű gyakorlatokba.

Új Kibervédelmi Katonai Koncepció[71] kiadása történt 2015 szeptemberében, a NATO struktúráján belül a kibervédelem keretrendszer meghatározása érdekében.

A NATO Számítógépes Eseménykezelő Képesség a NATO-rendszereket védi központosított, folyamatos (round-the-clock) kibervédelmi támogatást nyújtva a NATO-helyszínek felé.

[70] The Secretary General's Annual Report 2014, „Cyber security" fejezet, 15. o.

[71] Military Concept for Cyber Defence.

A NATO Kommunikációs és Információs Ügynökség[72] a monsi NATO Számítógépes Incidenskezelő Képesség, Technikai Központon (Technical Centre) keresztül felelős a NATO szintű technikai jellegű kibervédelmi és információvédelmi[73] támogatásért. Kezeli és jelenti az incidenseket, terjeszti a fontos incidensekkel kapcsolatos információkat a rendszer-, a biztonsági menedzsmentek és a felhasználók felé.

Az évben megtörtént a kibervédelmi képességi célkitűzések integrálása a NATO védelmi tervezési folyamatba. Az EU-val és az EBESZ[74]-szel szoros az együttműködés, különösen a kiberfenyegetésekkel kapcsolatos információmegosztás és a bizalomerősítő rendszabályok[75] kialakítása a kibertérben területeken.[76]

2015-ben egy NATO-híradás számol be a NATO Kiber Gyorsreagáló Csoport (2013-as) felállításáról. Cél a kibertámadást elszenvedő NATO-nemzetek, -létesítmények számára történő segítségnyújtás.

A kibertámadások pusztító következményekkel járhatnak, amelyek olyan súlyosak is lehetnek, mint a hagyományos támadások bombákkal és harckocsikkal. A csoport minden szükséges felszereléssel rendelkezik: számítógépes és telekommunikációs eszközök, behatolásérzékelők, műszaki elemzés (távolról vagy az érintett rendszeren), sérülékenységvizsgálat, hálózatbiztonság. A csoport nem egy hétköznapi kibervédelmi probléma vagy napi szintű kibertámadások megoldására alakult, a bevetés soha nem tervezett – ez a végső megoldás.[77]

Egy korábbi híradás szerint a gyorsreagáló csoport aktivizálása szabályozott. Bármely NATO-tagország, amely jelentős kibertámadást szenved el, igényelheti a NATO segítségét. A kérelmet a Kibervédelmi Menedzsment Felügyelet bírálja el.

A NATO-n kívüli országokból érkező kérelmeket az Észak-atlanti Tanácsnak kell jóváhagynia.[78]

A *NATO 2016-os varsói csúcsértekezlete* a publikáció elején már idézett követelmény mellett megállapítja, hogy a kibertámadások egyértelmű kihívást jelentenek a szövetség biztonsága szempontjából, és ugyanolyan károsak lehetnek a modern társadalmakra, mint a hagyományos támadások.

Walesben megállapodás történt, hogy a kibervédelem a NATO alapvető feladatának, a kollektív védelemnek része.

[72] NATO Communications and Information Agency – NCIA.

[73] Information Assurance.

[74] Európai Biztonsági és Együttműködési Szervezet (EBESZ). Organisation for Security and Co-operation in Europa (OSCE).

[75] Confidence-building measures.

[76] The Secretary General's Annual Report 2015, „Cyber Security" fejezet, 23. o.

[77] Men in black – NATO's cybermen (https://www.nato.int/cps/en/natohq/news_118855.htm).

[78] NATO Rapid Reaction Team to fight cyber attack (https://www.nato.int/cps/en/natohq/news_85161.htm).

Varsóban a szövetség megerősítette a védelmi mandátumot, és a kiberteret olyan műveleti területnek ismerte el, amelyben a NATO-nak ugyanolyan hatékonyan kell védenie önmagát, mint a levegőben, a szárazföldön és a tengereken.

A dokumentum szerint a szövetség megerősíti az elkötelezettséget, hogy a nemzetközi joggal – beleértve az ENSZ Alapokmányt, a nemzetközi humanitárius jogot és az emberi jogokat – összhangban jár el. A szövetség továbbra is a visszafogottság elvét fogja követni, és támogatni fogja a nemzetközi béke, biztonság és stabilitás fenntartását a kibertérben.

A szövetség üdvözli a felelős állami magatartás önkéntes nemzetközi normáival és a kibertérrel kapcsolatos bizalomépítő intézkedésekkel kapcsolatos munkát.

A szövetségesek a Kibervédelmi Kötelezettségvállalással egyértelműen jelezték, hogy prioritásként kezelik a nemzeti hálózataik és infrastruktúráik kibervédelmének megerősítését. Minden szövetséges tiszteletben tartja felelősségét az ellenálló képesség és a kibertámadásokra adott gyors és hatékony válaszadás növelése érdekében, beleértve a hibrid összefüggéseket is.

A NATO készen áll arra, hogy segítsen egy szövetségest a hibrid kampány bármely szakaszában. A kollektív védelem részeként a szövetség és a szövetségesek készen fognak állni a hibrid hadviselés elleni küzdelemre.[79]

A 2016-os NATO Kibervédelmi Kötelezettségvállalás alapján a szövetséges állam- és kormányfők ígéretet tesznek, hogy a szövetség lépést tart a kiberfenyegetettség gyorsan fejlődő környezetével, és a nemzetek képesek lesznek megvédeni magukat a kibertérben, mint a levegőben, szárazföldön és a tengeren.

A szövetségesek megerősítik nemzeti felelősségüket a nemzeti infrastruktúrák és hálózatok kibervédelmének fokozásában, valamint elkötelezettségüket a szövetséges biztonság és kollektív védelem oszthatatlansága mellett, összhangban a Walesben elfogadott NATO Megerősített Kibervédelmi Politikával.

A szövetségesek megerősítik a nemzetközi jog alkalmazhatóságát a kibertérben, és elismerik az érintett nemzetközi szervezetekben végzett munkát, többek között a felelős állami magatartás önkéntes normái és a kibertérben a bizalomépítő intézkedések terén.

A szövetséges állam- és kormányfők ígéretet tesznek arra, hogy prioritásként megerősítik, fokozzák a nemzeti hálózatok és infrastruktúrák kibervédelmét. A NATO kibervédelmi képességeinek folyamatos adaptálásával együtt – a NATO hosszú távú alkalmazkodásának részeként – ez megerősíti a szövetség kibervédelmét és általános ellenálló képességét. Kötelezettségvállalási célok:

1. A képességek legszélesebb skálájának fejlesztése a nemzeti infrastruktúrák és hálózatok védelme érdekében; különösen a kibervédelem legmagasabb stratégiai szintű kezelése a védelemmel kapcsolatos szervezeteken belül, a kibervé-

[79] Warsaw Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8–9 July 2016; 70–72.

delem további integrálása a műveletekbe és a képességek kiterjesztése a telepíthető hálózatokra.
2. Nemzeti szintű, megfelelő források elkülönítése a kibervédelmi képességek megerősítése érdekében.
3. A nemzeti kibervédelemért felelős szervezetek közötti kooperáció erősítése, az együttműködés mélyítése és a bevált gyakorlatok cseréje érdekében.
4. A kiberfenyegetések megértésének fejlesztése, beleértve az információmegosztás és a vizsgálatok fejlesztését.
5. Az alapvető kiber higiéniához szükséges szakértelem és tudatosság növelése egészen a fejlett és robosztus kibervédelmi szint biztosításáig nemzeti szinten a szükséges felelős szervezeteknél.
6. A kibervédelmi erők oktatásának, képzésének és gyakorlásának elősegítése, az oktatási intézmények fejlesztése a szövetségen belüli bizalom és tudásbázis kiépítése érdekében.
7. Az elfogadott kibervédelmi kötelezettségvállalások végrehajtásának felgyorsítása, beleértve azokat a nemzeti rendszereket is, amelyek a NATO felé nyújtanak szolgáltatást (és ezáltal függőséget jelentenek).

A szövetségesek a Kötelezettségvállalást évente áttekintik.[80] Az évek során kialakult a vállalással kapcsolatos eljárásrend, ami az éves változások közlése mellett szervezett konzultációt biztosít, illetve a további részben látható éves konferencia ezen túlmenően is információcsere-lehetőséget teremt a szövetségesek között és a szövetséges–NATO viszonylatban is.

A 2016-os év eseménye annak megerősítése, hogy a kibertámadások növekvő fenyegetésével szemben a NATO és az EU hasonló kihívásokkal néz szembe a hálózatok védelme területén. Annak érdekében, hogy mindkét szervezet jobban megfeleljen a kihívásnak, technikai megállapodás született a NATO Számítógépes Eseménykezelő Központ (NCIRC) és az EU Számítógépes Eseménykezelő Központ[81] között. A technikai megállapodás keretet biztosít az eseménykezelő szervezetek közötti információcseréhez és a bevált gyakorlatok megosztásához. *Kiterjed a konkrét kiberfenyegetésekkel kapcsolatos információcserére, valamint a műszaki eljárásokra, a hálózatok konfigurálására és az iparággal való partnerségre vonatkozó bevált gyakorlatok megosztására.*[82]

A *NATO állam- és kormányfők 2016-os Varsói Nyilatkozata* szerint a szövetségesek elkötelezték magukat, hogy továbbra is fokozzák ellenálló képességüket a teljes

[80] Cyber Defence Pledge, 1, 3, 5. o. (https://www.nato.int/cps/en/natohq/official_texts_133177.htm).

[81] Computer Emergency Response Team (CERT-EU).

[82] NATO and the European Union enhance cyber defence cooperation (https://www.nato.int/cps/en/natohq/news_127836.htm).

spektrumú fenyegetésekkel szemben – beleértve a hibrid fenyegetéseket –, bármilyen irányból is érkezzenek azok.

Növelik az ellenálló képességet a robusztus, rugalmas és interoperábilis katonai képességekbe történő befektetéssel, összhangban a NATO ambíciói szintjével és a walesi csúcstalálkozón tett védelmi beruházásokra tett ígéretekkel.

Védeni fogják a katonai ellátási láncokat, és azon dolgoznak, hogy adott esetben nemzeti erőfeszítések és multinacionális együttműködés révén kezeljék az orosz forrásokból származó örökölt katonai felszerelések meglévő függőségeit.

Kiemelten megerősítik és fokozzák nemzeti infrastruktúrák és hálózatok védelmét a növekvő fenyegetés és a nagy bonyolultságú kibertámadások ellen.[83]

A *NATO-főtitkár 2016-os évre vonatkozó jelentése szerint* a kiberfenyegetések és támadások egyre gyakoribbak, kifinomultabbak és károsabbak. Ezek a támadások leállíthatják az infrastruktúrákat, aláásható a demokratikus rendszereket, és hatással lehetnek a katonai műveletekre.

A változó biztonsági környezet fényében a kibervédelem kulcsfontosságú prioritássá vált. A technikai lehetőségből egy olyan műveleti területté fejlődött, ahol a NATO-nak ugyanolyan hatékonyan kell fellépnie, mint a szárazföldön, a levegőben vagy a tengeren.

Más szervezetekhez hasonlóan a NATO-nak is gyorsan változó kibervilággal kell szembenéznie, ahol egyre gyakoribbak a konkrét és célzott támadások. Az ilyen támadások észlelése a hatalmas mennyiségű hagyományos online tevékenység közepette kifinomult képességeket és szakértelmet igényel.

A NATO varsói csúcstalálkozóján a szövetségesek két fontos döntést hoztak a változó kiberfenyegetési kép[84] ellensúlyozása érdekében.

A szövetségesek a kiberteret műveleti területként ismerték el, ahol a NATO-nak meg kell védenie magát, hasonlóan a légi, földi vagy tengeri műveletekhez. Így a NATO-struktúra képes lesz kiemelt figyelmet fordítani a missziók és műveletek védelmére a kiberfenyegetések ellen, koncentrálva a kiberrel kapcsolatos képzésekre, illetve kétséges vagy sérült biztonságú kiberkörnyezetben történő művelettervezésre. Ez nem jelent változást a NATO-missziók mandátumaiban, melyek továbbra is védelmi jellegűek maradnak, követve a nemzetközi normák által meghatározottakat.

A szövetségesek kötelezettséget vállaltak a kibervédelmi képességek prioritással történő megerősítésére és kiterjesztésére – beleértve a nemzeti infrastruktúrák és hálózatok védelmét is.

Technikai eredmény, hogy 19 nemzet frissítette a NATO-val történő együttműködési megállapodást, illetve e mellett a NATO Számítógépes Incidenskezelő Ké-

[83] Commitment to enhance resilience Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, 8–9 July 2016, 1, 6, 7.

[84] Cyber threat landscape.

pesség és az EU Számítógépes Eseménykezelő Központ[85] együttműködési megállapodást kötött.[86]

2016-os nemzeti esemény, hogy a honvédelmi ágazati elektronikus információbiztonsági hatósági felügyeleti feladatok elkülönültek az állami és önkormányzati szervezetekre vonatkozó szabályozásban, és a KNBSZ-főigazgató hatáskörébe kerültek.[87]

Az évben megújult a korábban említett, 2010-ben megkötött NATO–magyar kibervédelmi együttműködési megállapodás. A kapcsolattartási feladatok ezzel a lépéssel a honvédelmi ágazathoz kerültek.

A „második generációs" együttműködési megállapodás fókuszában a védelempolitikai szintű kapcsolattartás mellett a szövetségesi együttműködést támogató, azonnali információcsere szükséglet áll. A szövetségi vagy magyar rendszereket ért incidensekről, sérülékenységekről szóló azonnali intézkedést kiváltó kölcsönös riasztások, tájékoztatások a technikai szintű, napi működés támogatását szolgálják. A NATO felől érkező adatok feldolgozás után a Nemzeti Kibervédelmi Intézet felé történő továbbítása biztosítja az érintett magyar kormányzati vagy egyéb szervezetek információkkal történő támogatását.[88]

A *2017-re vonatkozó NATO-főtitkári éves jelentés* megállapítja, hogy a mai világban a kiberfenyegetések egyre kiterjedtebbek, kifinomultabbak és károsabbak, mint valaha. Egy kibertámadás legrosszabb esetben veszélyeztetheti egy ország kritikus infrastruktúráját, megbéníthatja kormányát, aláásható a demokratikus rendet, vagy befolyásolja a fegyveres erők műveleti hatékonyságát.

A NATO fokozta a szövetség kommunikációs hálózatainak és információs rendszereinek védelmét, az egyes szövetségesek támogatását a nemzeti kibervédelemben, illetve a testre szabott tanácsadást a partnerek számára.

2017-ben növekedett a választék a szolgáltatások megzavarására alkalmazott technikákban, a kémkedésben vagy a szövetség reputációjának megsértésében, beleértve a NATO-webhelyek szolgáltatásainak megszakítására tett kísérleteket is.

A NATO folyamatos védelmet nyújt hálózatok számára a NATO Kommunikációs és Információs Ügynökség által biztosítva, illetve gyors reagálású kibervédelmi csoportokat tart készenlétben, rövid reagálási idejű telepíthetőséggel (a NATO-infrastruktúra védelme és a szövetségesek támogatása érdekében).

[85] EU Computer Emergency Response Team – CERT.

[86] The Secretary General's Annual Report 2016, „Cyber Defence" fejezet, 24. o.

[87] 22/2016. (II. 17.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet módosításáról, 1. §.

[88] Hungary signs new MoU on cyber defence cooperation; (https://nicp.nato.int/hungarysigns-new-mou-on-cyber-defence-cooperation/index.html).

Az évben a NATO illetékes szervezetei folytatták a tervek, képzések pontosítását a missziók és műveleteket kiberfenyegetések elleni védelme érdekében a varsói csúcstalálkozón a kibertérműveleti területté történő kinyilvánítás követeséként, mely szerint a NATO-nak képesnek kell lenni megvédeni önmagát, akárcsak a levegőben, a szárazföldön és a tengeren.

A kibervédelem szerepet játszik a NATO parancsnoki struktúra adaptálásáról szóló egyeztetésekben, a szövetségesek nemzeti kiberképességeinek a NATO-műveletekbe történő legjobb integrálása érdekében. Ez egy új kiberműveleti központ kialakítására vonatkozó lehetőség vizsgálatát jelenti. Mint minden más műveleti területen, a NATO működése a kibertérben is védelmi jellegű, arányos műveleteket alkalmazó (proportionate), és teljeskörűen összhangban áll a nemzetközi joggal.

A robusztus kibervédelem megköveteli a szövetségtől, hogy lépést tartson a technológiai változások gyors ütemével. A NATO konzultál, együttműködik, és valós idejű információkat oszt meg a kiberfenyegetésekről szövetségeseivel, partnereivel és más nemzetközi szervezetekkel, például az EU-val, valamint az iparral.

Például a 2017-es nagy horderejű WannaCry és NotPetya kibertámadások során a NATO kibervédelmi szakértői gyorsan egyeztettek a szövetségesekkel, az EU-partnerekkel, az ipari partnerekkel, hogy legfrissebb képet kaphassanak a bonyolult és gyorsan történő eseményekről.[89]

A 2017-es év nemzeti eseménye a korábban jelzett honvédelmi felelősségi kör kijelölésének folytatásaként, hogy a jogszabályokban meghatározott szakfeladatok végrehajtása érdekében megjelent az eseménykezelésre, sérülékenységvizsgálatra és hatósági feladatokra vonatkozó HM-utasítás.[90]

A *NATO 2018-as brüsszeli csúcsértekezlete* megállapítása szerint a szövetség veszélyes, előrejelezhetetlen és képlékeny (fluid) biztonsági környezetben, tartós fenyegetésekkel és kihívásokkal találkozik minden stratégiai irányból, állami és nem állami szereplőkkel, katonai erővel, terroristákkal, kiber- és hibrid támadásokkal szemben – beleértve a megtévesztő kampányokat[91] és a kártékony célú kibertevékenységeket.[92]

A szövetség folytatja a hírszerzés optimalizálását, elősegítve a NATO időbeli és relaváns döntés előkészítését és műveleteit, beleértve az előrejelzést és a hírszerzési adatok megosztását, kiemelten a terrorizmus, hibrid és kiberterületeken.

A kibervédelem része a NATO kollektív védelmének. Ugyanolyan hatékonyan kell működni a kibertérben, mint a levegőben, a szárazföldön és a tengereken, meg-

[89] The Secretary General's Annual Report 2017, „Investing in Cyber Defence" fejezet, 19–20. o.

[90] 15/2017. (IV. 28.) HM utasítás a honvédelmi célú elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóság és a honvédelmi ágazati elektronikus információbiztonsági eseménykezelő központ feladatainak végrehajtásáról, valamint a sérülékenységvizsgálat lefolytatásának szabályairól.

[91] Disinformation campaigns.

[92] Malicious cyber activities.

erősítve és támogatva a szövetség általános elrettentési és védelmi jellegét. Ezért folytatni kell a kibertérműveleti területként történő alkalmazásának megvalósítását.

A szövetségesek megállapodtak az önkéntesen biztosított kiberhatások[93] erős politikai felügyelet keretében történő integrálásában a szövetség műveleteibe és misszióiba.

Megerősítve a NATO védelmi jellegét, a szövetségesek elhatározták, hogy a képességek teljes skáláját alkalmazzák az elrettentés és a védelem érdekében a kiberfenyegetések teljes spektruma ellen, beleértve a hibrid kampány részeként végrehajtottakat is.

További lépésként meg kell erősíteni a hírszerzés által vezérelt helyzetismeretet[94] a NATO döntéshozatalának és műveleteinek támogatása érdekében. Olyan intézkedéseket kell kidolgozni, amelyek alapján növekedjenek a költségei azoknak, akik ártani akarnak a szövetségnek.

A szövetségesek adott esetben fontolóra vehetik a rosszindulatú kiberaktivitás betudását (attribution) és az arra történő koordinált válaszadást, ezzel egyidejűleg megerősítve, hogy a betudás szuverén nemzeti hatáskör.

A szövetség megerősíti kötelezettségvállalását abban, hogy cselekvései összhangban lesznek a nemzetközi joggal – beleértve az ENSZ Alapokmányát, a nemzetközi humanitárius jogot és az emberi jogokat –, ahol azok alkalmazása szükséges.

A szövetség támogatja továbbá a munkát a kibertérben a nemzetközi béke és biztonság fenntartása, valamint a stabilitás elősegítése és a konfliktusok kockázatának csökkentése érdekében, felismerve, hogy a normákon alapuló (norms-based), kiszámítható és biztonságos kibertér mindenki számára hasznos lehet.

A szövetség Kibertérműveleti Központot[95] alakít Belgiumban, helyzetismeretképet és koordinációt biztosítva a NATO-műveletekhez a kibertérben.[96]

A *NATO-főtitkár 2018-as évre vonatkozó jelentése* szerint az ellenálló képesség a sokkszerű hatásokkal szemben történő ellenállást, illetve visszaállítás képességét jelenti természeti katasztrófa, hagyományos fegyveres támadás vagy hibrid művelet esetén. A szövetségesek ellenálló képessége és civil felkészülése létfontosságú a NATO kollektív védelme és biztonsága érdekében. Az ellenálló képesség a védelem első vonala.

A fegyveres erők erősen függenek a civil infrastruktúráktól és képességektől, beleértve az élelmiszert és vizet, kommunikációt és szállítást. Az országok civil infrastruktúrájának ellenálló képessége ugyanolyan fontos, mint a katonai infrastruk-

[93] Sovereign cyber effects.

[94] Intelligence-led situational awareness.

[95] Cyberspace Operations Centre.

[96] Brussels Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11–12 July 2018; 1, 13, 20, 29.

túrák, így a civil felkészülés alapvető fontosságú a NATO elrettentési és védelmi képessége szempontjából.

A NATO brüsszeli csúcstalálkozóján (2018) a szövetségesek kinyilvánították, hogy a kibervédelem a NATO kollektív védelmének, alapfunkciójának része, így a szövetségnek hatékonyan kell működnie a kibertérben, mint azt teszi a levegőben, szárazföldön és tengereken. A NATO elsődleges prioritása marad a saját hálózatok védelme, világszerte.

2018-ban a szövetségesek a Kibervédelmi Kötelezettségvállalás mentén folyamatosan dolgoztak a saját nemzeti hálózatok ellenálló képességének növelésén.

A NATO-nak nincs saját offenzív kiberképessége, és nincs terv ilyen képesség kifejlesztésére. Más műveleti területekhez hasonlóan a NATO a szövetségesek által felajánlott képességekkel fog rendelkezni. A 2017-es politikai irányelvek szerint néhány szövetséges nyilvánosan felajánlotta nemzeti kiberkapacitásának integrálását szövetségi műveletekbe és missziókba (szükség esetén).

A kibervédelem fontos együttműködési terület az EU-val. A NATO-és EU-törzsek növekvő számban vesznek részt közösen gyakorlatokon[97] melyek kiberelemeket is tartalmaznak.

A 2016-os közös deklaráció óta a két szervezet kiterjedt, részletekre kitérő információcserét folytat a kiberkrízisek kezelésének megközelítéséről.[98]

A 2018-as párizsi Kibervédelmi Kötelezettségvállalás Konferencián a NATO-főtitkár összefoglalta a közelmúlt legfontosabb történéseit. Rámutatott, hogy 2014-ben a NATO vezetői egyetértettek abban, hogy egy kibertámadás elindíthatja az Alapszerződés 5. cikkét. Ennek értelmében egy szövetséges elleni támadást minden szövetséges elleni támadásként kell kezelni. Hagyományosan az 5. cikk szerinti támadás harckocsikkal, repülőgépekkel és katonákkal történik. Most kibertámadás formájában is megvalósulhat. A kiber a tevékenységek középpontjába került.

2016-ban a NATO vezetői a kiberteret „műveleti területnek (domain)" azonosították a szárazföld, a tenger és a levegő mellett. Ez azt jelenti, hogy felül kell vizsgálni mindent, a legmagasabb szinttől a legalacsonyabbig.

Ugyancsak 2016-ban a nemzetek vezetői egyetértettek a Kibervédelmi Kötelezettségvállalással. Ennek eredményeként kevesebb, mint két év alatt szinte minden szövetséges korszerűsítette a kibervédelmet.

Az új parancsnoki struktúra részeként megalakult a NATO Kibertérműveleti Központ. Megkezdődött a kiber integrálása a tervezésbe és a műveletekbe. Üdvözletes, hogy néhány szövetséges nemzeti kiberképességeivel hozzájárul a NATO-műveletekhez.

[97] NATO's Cyber Coalition and the EU's Parallel and Coordinated Exercise.

[98] The Secretary General's Annual Report 2018, „A More Resilient NATO" és „Securing Cyberspace" fejezetek, 22, 24. o.

A NATO gyorsreagálású csoportjai[99] készenlétben állnak a szövetségesek segítésére a nap 24 órájában.

A súlyos kibertámadásokra a szövetség választ tud adni akkor is, ha azok nem lépik át az 5. cikk szerinti küszöböt. De bármi legyen is a válasz, a NATO továbbra is a visszafogottság elvét (restrain principle) fogja követni, és a nemzetközi jognak megfelelően jár el.

Gyakran nehéz tudni, hogy ki áll a támadás mögött – legalábbis kezdetben. A betudás (attribution) fontos szerepet játszhat a jövőbeli támadások elrettentésében is.[100]

A 2018-as év nemzeti eseménye a magyar csatlakozás a Károskód Információmegosztó Platformhoz, ami folyamatos technikai információcsere-lehetőséget biztosít az eseménykezelés támogatása érdekében.

A megalakult NATO Kibertérműveleti Központ kezdő csapatában egy magyar tábornok – Vass Sándor – látott el vezetői beosztást, ami egyértelmű büszkesége lehet a nemzeti színeknek.

A 2019-es londoni csúcsértekezlet deklarációja szerint a szövetség folytatja a társadalom, a kritikus infrastruktúra és az energiabiztonság területén az ellenálló képesség növelését.

A NATO és a szövetségesek elkötelezettek a saját hatáskörön belül a kommunikáció biztonságában (beleértve az 5G technológiát), felismerve a rendszerek biztonságának és ellenálló képességének fontosságát.

A szövetség fejleszti eszközeit a kibertámadások elleni válaszokra, és erősíti képességeit felkészülés, elrettentés és a hibrid taktikák elleni védelem területein, melyek a társadalom és a biztonság aláaknázását célozzák.[101]

A *2019-re vonatkozó NATO-főtitkári éves jelentés* szerint a kibervédelem a NATO kollektív védelemre vonatkozó alaprendeltetés része. A súlyos hatásokkal járó kibertámadások kiválthatják az 5. cikkely alkalmazását.

A NATO-tagállamok elsődleges felelőssége a nemzeti kibervédelem – mivel a NATO kibervédelme az összekapcsolásokon alapul –, így az olyan erős, mint a leggyengébb láncszem. Emiatt a szövetségesek kötelezettséget vállaltak, hogy a kibervédelem megerősítését prioritással kezelik. A NATO támogatni fogja szövetségeseit ebben az erőfeszítésben.

A NATO szervezeti struktúrája modernizálásának keretében a Kibertérműveleti Központ elérte a műveleti képességét. A szövetségesek egyetértettek abban, hogy saját kibertérműveleti képességeikkel támogatják a NATO műveleteit, így számos

[99] Cyber Rapid Reaction Teams.

[100] Speech by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference (Ecole militaire, Paris) (2018).

[101] London Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in London 3–4 December 2019, 6.

nemzet felajánlotta már képességeit. A szövetségesek teljes mértékben megtartják felügyeleti jogaikat saját nemzeti kiberműveleti képességeik felett a NATO-missziók és -műveletek támogatása során.

A NATO folytatólagosan támogatta a szövetségeseket a Kibervédelmi Kötelezettségvállalás teljesítésében a három évvel korábban, Varsóban tett vállalás szellemében a nemzeti kiber ellenálló képesség erősítése érdekében.

A szövetségesek fejlesztették jogi és szervezeti keretrendszerüket, folyamatosan erősítették pénzügyi és humánerőforrásaikat a kiberfenyegetések ellensúlyozása érdekében.[102]

A *2019-es londoni Kibervédelmi Kötelezettségvállalás Konferencián* a NATO- főtitkár elmondta, a kibertámadások egyre gyakoribbak, összetettebbek és pusztítóbbak. A NATO nem immunis. Mindennap érzékelhetők gyanús események a NATO kiberrendszerei ellen.

A kiberfenyegetések az új technológiák fejlődésével veszélyesebbé válnak, mint például a mesterséges intelligencia, a gépi tanulás és a deep fakes.[103] Ezek a technológiák alapvetően megváltoztatják a hadviselés jellegét, legalább annyira, mint az ipari forradalom. A NATO alkalmazkodik ehhez az új valósághoz.

A NATO vezetői megállapodtak abban, hogy egy kibertámadás aktivizálhatja az Alapszerződés 5. cikkét. E szerint egy szövetséges elleni támadást mindenki elleni támadásként kell kezelni. A NATO a kiberteret katonai műveleti területnek jelölte ki, a szárazföld, a tenger és a levegő mellett.

A 2018-as brüsszeli csúcstalálkozón megállapodás született a Kibertérműveleti Központ létrehozásáról. Megállapodás történt a nemzeti kiber (vagy offenzív) képességek szövetség műveleteibe és misszióiba történő integrálásáról.

A Kibervédelmi Kötelezettségvállalás segíti a szövetségeseket a védelem fokozásában. A szövetségesek megerősítették kiberképességeiket, javították jogi és intézményi kereteiket, növelték a kiberfenyegetések kezelésére fordított erőforrásokat – munkaerőt és pénzeket.

Ahhoz, hogy az elrettentés teljes hatást érjen el, a potenciális támadóknak tudniuk kell, hogy a NATO nem korlátozódik a kibertérben történő válaszadásra, amikor a kibertérben éri támadás. A rendelkezésre álló képességek teljes skáláját tudjuk és fogjuk alkalmazni.

A NATO 70 éve tartja biztonságban az embereket a fizikai világban. Most a NATO-nak ugyanezt kell tennie a kibervilágban is. Ehhez meg kell tartani a technológiai előnyt, biztosítani kell az új technológiák lehetséges előnyeinek kiaknázását, a lehetséges kockázatok minimalizálása mellett.

[102] The Secretary General's Annual Report 2019, „Cyberspace as Part of NATO's Core Task of Collective Defence" fejezet, 27. o.

[103] Deep fakes: *pontos fordítás még nem alakult ki, jelentése: mesterséges intelligencia segítségével módosított (hamisított) médiatartalom.*

A kiber túlmutat a technológián. A technológia mögött álló emberek ugyanolyan fontosak. A jövőbeli kiberspecialistákból („future cyber defenders") erős és sokféle munkaerőt kell építeni.

Gondoskodni kell arról, hogy a készségek rendszeres gyakorlatok révén bevethetők (élesek) legyenek, ahogyan az a NATO Cyber Coalition – a világ egyik legnagyobb kibervédelmi gyakorlata – révén történik.[104]

2019-ben nemzeti szempontból jelentős esemény a Magyar Honvédség Parancsnokságának megalakulása. A parancsnokságon belül kibervédelmi szakfeladatok ellátására a haderőnemi szemlélőségek rendjében kijelölt szervezeti elem jelenik meg, a haderőnemi szemlélő (kibervédelmi). A funkció részletezése nélkül megállapítható, hogy a korábbi, kibervédelmi szervezetépítési események mellett ez az első olyan lépés, ami a Honvédségnél a kibertérben rejlő lehetőségek katonai megvalósítását célozza.

A *NATO 2020-ra vonatkozó főtitkári éves jelentése* szerint a biztonságos kibertér elengedhetetlen a szövetség minden tevékenységéhez. Ezért a kibervédelem része a NATO kollektív védelem alapvető feladatának. A NATO világossá tette, hogy egy súlyos kibertámadás a Washingtoni Szerződés 5. cikkének alkalmazásához vezethet.

A szövetség folytatja a doktrínák kidolgozását, valamint kiképzéseket és gyakorlatokat annak biztosítására, hogy a kibertérben ugyanolyan hatékony legyen, mint a szárazföldön, a levegőben és a tengeren. 2020-ban megjelent az első kiberdoktrína. Ez fontos lépés a kibertérbeli műveletekre vonatkozó útmutatáshoz.

Az éves NATO Cyber Coalition gyakorlat az aktuális fenyegetésekből merítve tesztelte a résztvevők valós idejű reakcióit a kiberincidensekre, például a titkosított hálózatok feltörésére, a kritikus infrastruktúra kommunikációs rendszereinek megzavarására és az okostelefonos alkalmazásokon keresztül történő kémkedésre.

A szövetségesek a 2016-os varsói csúcstalálkozón vállalt kötelezettségüknek megfelelően folytatták nemzeti kiberellenálló képességük fokozását. Stratégiai iránymutatások kiadásával és felülvizsgálatával erősítették kiberellenálló képességüket, beleértve az ellátási láncokat érintő kiberkockázatok kezelését, a szervezeti reformok végrehajtását és a képzésbe való befektetést.

Az információmegosztás soha nem volt ennyire kritikus. A NATO Kommunikációs és Információs Ügynökség a Kiber Együttműködési Hálózaton[105] keresztül továbbra is elősegítette a NATO-szövetségesek közötti kiberfenyegetésekkel és -incidensekkel kapcsolatos információcserét.[106]

[104] Remarks by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference, London.

[105] Cyber Collaboration Network.

[106] The Secretary General's Annual Report 2020, „Deterrence and Defence in Cyberspace" fejezet, 23–24. o.

A NATO-főtitkárhelyettes egy 2020-as szakmai konferencián történt előadása szerint sok évszázadon át a biztonság a szárazföldön és a tengeren jelentkező fenyegetések kezelését jelentette, az elmúlt évszázadtól már a levegőben lévő fenyegetések is megjelentek.

A technika számos közelmúltbeli fejlődése átalakítja a fenyegetéseket, amelyek ma több formát is ölthetnek és egyszerre több irányból is érkezhetnek. Közelről kézi módszerekkel vagy nagyon messziről, külső közvetítéssel. Emberektől vagy személyzet nélküli rendszerekből. Az űrből vagy a kibertérből. Ezeket a trendeket fokozzák az olyan gyorsan fejlődő technológiák, mint a mesterséges intelligencia és a robotika.

Alkalmazkodni kell annak érdekében, hogy szövetség felkészült legyen a fenyegetések kezelésére mind a fizikai, mind a virtuális világban. A kiberfenyegetések ezek közé tartoznak, melyek egyre gyakoribbak, összetettebbek és pusztítóbbak.

Az elmúlt években fontos döntések születtek a NATO jobb „kiberkészenléte" („cyber-ready") és „kiberbiztonságossá" („cyber-secure") tétele érdekében.

Megállapodás született, hogy egy kibertámadás is elindíthatja az Alapszerződés 5. cikkét. Ahol egy szövetséges elleni támadást mindenki elleni támadásként kezelnek.

Megtörtént a kibertér katonai műveleti területként történő azonosítása a szárazföld, a tenger és a levegő mellett. Az űr is műveleti területté vált a vezetők tavaly londoni döntése szerint.

Szintén megállapodás történt arról, hogy katonai vezetési struktúra központjában egy Kibertérműveleti Központ alakuljon.

További megállapodás volt, hogy a nemzeti kiberhatásokat – vagy offenzív kiberműveleteket – („offensive cyber") integrálni kell a szövetség műveleteibe és misszióiba.

Megszületett a Kibervédelmi Kötelezettségvállalás, ami elengedhetetlen a kiberfenyegetésekkel szembeni ellenálló képességek fokozásához.

Júniusban a NATO-szövetségesek közös nyilatkozatot adtak ki, amelyben elítélik a pandémiával összefüggésben zajló destabilizálást és rosszindulatú kiberaktivitásokat. A nyilatkozat felszólított továbbá a nemzetközi jogi normák tiszteletben tartására és a felelős állami viselkedésre a kibertérben.[107]

2020-as nemzeti vonatkozású esemény, hogy hazánk korlátozás nélküli bevezetéssel ratifikálta a NATO Kiberműveleti Doktrínát. Ez a lépés biztosítja az interoperabilitást a NATO-missziók támogatása során, továbbá a nemzeti–NATO vagy szövetséges–szövetséges típusú együttműködés során a legfontosabb kérdésekben a doktrína fogalmi rendszerén belüli közös tevékenységet.[108]

[107] Speech by NATO Deputy Secretary General Mircea Geoană at the CYBERSEC GLOBAL 2020 virtual conference (https://www.nato.int/cps/en/natohq/opinions_178335.htm).

[108] NATO Cyber Operations Doctrine (AJP 3.20). 42/2020. HM utasítás egyes NATO egységesítési jelzések elfogadásáról, 5. §.

A *NATO 2021-es brüsszeli csúcsértekezlete* megállapítása szerint a szövetség biztonságát fenyegető kibertámadások egyre összetettebbek, pusztítóbbak, kényszerítőbbek és gyakoribbak. Ezt szemléltetik a nemrég történt kritikus infrastruktúrákat és demokratikus intézményeket célzó zsarolóvírus (ransomware) incidensek és egyéb rosszindulatú kiberaktivitások, melyek rendszerszintű, jelentős károkat okozhatnak.

A változó kihívásnak való megfelelés érdekében megtörtént a NATO Átfogó Kibervédelmi Politika[109] elfogadása, ami támogatja a NATO három alapvető feladatát, az általános elrettentést, a védelmi jelleget és az ellenálló képesség fokozását.

A NATO védelmi mandátumát megerősítve a szövetség eltökélt szándéka, hogy minden időben a képességek teljes skáláját aktívan alkalmazza az elrettentés, a teljes spektrumú kiberfenyegetések elleni védelem érdekében – beleértve a hibrid kampányok részeként lebonyolított műveleteket –, összhangban a nemzetközi jog követelményeivel.

A szövetségesek megerősítik, hogy az Észak-atlanti Tanács eseti alapon dönt arról, hogy a kibertámadás mikor vezet az 5. cikk alkalmazásához. A szövetségesek elismerik, hogy a jelentős, rosszindulatú kibertevékenységek halmozódó hatása[110] bizonyos körülmények között fegyveres támadásnak tekinthető.

A szövetség továbbra is elkötelezett a nemzetközi joggal összhangban történő cselekvésre, beleértve az ENSZ Alapokmányát, a nemzetközi humanitárius jogot és a nemzetközi emberi jogi jogszabályokat, ahol azok alkalmazhatók.

A szövetség elősegíti a szabad, nyitott, békés és biztonságos kibertér kialakítását, és további erőfeszítéseket fog tenni a stabilitás fokozása és a konfliktusok kockázatának csökkentése érdekében a nemzetközi jog támogatásával és a felelős állami viselkedés önkéntes normáival[111] a kibertérben.

A NATO, ha szükséges, költségeket számít fel azoknak, akik sérelmet okoznak a szövetségnek. A válasznak nem szükséges a kiberterületre korlátozódnia.

Növelni kell a helyzetismeretet a NATO-döntéshozatal támogatása érdekében.

A Kibervédelmi Kötelezettségvállalás adoptálása után öt évvel a szövetség továbbra is elkötelezett az erős nemzeti kibervédelem támogatásában, prioritásként. Folytatódik a „kibertér mint műveleti terület" elv megvalósítása.

Erős politikai felügyelet keretében növelni kell a szövetségesek által önkéntesen biztosított szuverén kiberhatások hatékony integrálását a kollektív védelembe, a szövetségi műveletekbe és missziókba.

A szövetség tovább törekszik a kölcsönösen előnyös és hatékony együttműködések kialakítására, beleértve a partnerországokat, a nemzetközi szervezeteket, az

[109] Comprehensive Cyber Defence Policy.

[110] The impact of significant malicious cumulative cyber activities.

[111] Voluntary norms of responsible state behaviour.

ipart és az oktatást, illetve folytatja az erőfeszítéseket a nemzetközi stabilitás fokozása érdekében a kibertérben.

A szövetség üdvözli a közelmúltban Portugáliában megnyílt NATO Kommunikációs és Információs Akadémiát.[112], [113]

A *NATO 2021-es Brüsszeli Ellenálló Képesség Megerősítéséről Szóló Kötelezettségvállalás*a nem kifejezetten a kibertérműveleteket célozza, ennél szélesebb és magasabb szintű követelményeket fogalmaz meg, melyeknél pontosan azonosítható a kibertérműveleti szakmai érintettség is. A vállalás szerint az ellenálló képesség nemzeti felelősség és kollektív kötelezettségvállalás.

A szövetségesek javaslatot dolgoznak ki az ellenálló képesség – mint célkitűzés – megállapítására, értékelésére, felülvizsgálatára és nyomon követésére, hogy irányítsák a nemzeti szinten kidolgozott ellenálló képességi célokat és végrehajtási terveket. Minden egyes szövetségesnek el kell döntenie, hogyan kell meghatározni a nemzeti ellenálló képességi célokat, és teljesíteni a végrehajtási terveket, lehetővé kell tenni, hogy ezt olyan módon tegyék, ami kompatibilis a nemzeti hatáskörökkel, struktúrákkal, folyamatokkal és kötelezettségekkel, – ahol szükséges – az EU-kötelezettségekkel.

Az ellenálló képességet fenyegető veszélyek és kihívások állami és nem állami szereplőktől erednek, különböző formákat öltenek, és különféle taktikákat és eszközöket használnak. Idetartoznak a hagyományos, nem hagyományos és hibrid fenyegetések és tevékenységek, a terrortámadások, a növekvő és egyre kifinomultabb rosszindulatú kibertevékenységek, az egyre szélesebb körben terjedő ellenséges információs tevékenységek, beleértve a dezinformációt, amelyek célja a társadalmak destabilizálása és közös értékek aláásása és beavatkozási kísérlet a demokratikus folyamatokba, a hatékony kormányzásba.

Fokozni kell az erőfeszítéseket az ellátási láncok biztosítása és diverzifikálása, a kritikus infrastruktúrák (szárazföldön, tengeren, űrben és a kibertérben) és kulcsfontosságú iparágak ellenálló képességének biztosítása érdekében, beleértve a káros gazdasági tevékenységeket.

Kezelni kell a fejlődő technológiák hatását, biztosítva a következő generációs kommunikációs rendszerek és a szellemi tulajdon védelmét.[114]

A *2021-re vonatkozó NATO-főtitkári éves jelentés* szerint az évben a kiberfenyegetések továbbfejlődtek. Megszaporodtak a megszakító jellegű (distruptive) és rosszindulatú kiberkampányok, beleértve az állami és nem állami szereplők által elkövetett zsarolóvírus-támadásokat is. Ezek a rosszindulatú támadások a kritikus infrastruktúrát és ellátási láncokat célozták a szövetséges és a partnerországokban.

[112] NATO Communications and Information Academy.

[113] Brussels Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 14 June 2021, 32.

[114] Strengthened Resilience Commitment (2021), 4, 5, 7, 8.

A kihívás megoldása érdekében a szövetségesek támogatták a NATO Átfogó Kibervédelmi Politika[115] kiadását. Ez mérföldkövet jelentett a NATO kibervédelemmel kapcsolatos megközelítésének meghatározásában a következő évtizedre.

A szövetségesek hangsúlyozzák, hogy a szövetséget érő kiberfenyegetések összetettek, pusztítóak, kényszerítőek és egyre gyakoribbá válnak, miközben a kibertér egyes kérdései vitatottak.

A szövetség eltökélt szándéka, hogy – a NATO védelmi mandátumával és a nemzetközi joggal összhangban – képességeinek teljes skáláját alkalmazza a kiberfenyegetések ellen és azok elrettentése érdekében, beleértve azokat is, melyek hibrid kampányok részeként történnek.

A hatékony kibervédelem átfogó megközelítést igényel, ami egyesíti a politikai, katonai és technikai szintű erőfeszítéseket.

A NATO-nak képesnek kell lennie arra, hogy megvédje hálózatait, zökkenőmentesen működjön a kibertérben, és elő kell mozdítania a normákon alapuló megközelítést a kibertérben. Ez megkívánja a szövetségesek közös helyzetismeretét, valamint a behatolások valós idejű észlelésének, megelőzésének és reagálásának képességét.

A kibertérben a szövetség csak annyira erős, amennyire a leggyengébb láncszem. A 2021-es csúcstalálkozón a szövetségesek egyetértettek abban, hogy az ellenálló képesség, valamint az új sebezhetőségek észlelésének, megértésének és az azokra való reagálásnak a képessége egyre fontosabbá válik.

A 2016-ban a varsói csúcstalálkozón elfogadott Kibervédelmi Kötelezettségvállalás továbbra is a nemzeti ellenálló képesség kiépítésének kulcsfontosságú eszköze. A Kötelezettségvállalás révén a szövetségesek azon dolgoznak, hogy fejlesszék a kibermunkaerőt, szakértőket toborozzanak olyan innovatív megközelítések révén, mint például a kibertartalékos programok, és befektetnek a kibervédelmi képességekbe és szakértelembe.

A NATO a védelmi erőfeszítéseket a kormány egészére kiterjedő megközelítéssel folytatja,[116] ami elismeri a katonaság, a kormány, az ipar és a tudományos élet szerepét az ellenállóképes kibervédelem megvalósításában.[117]

A *NATO-főtitkárhelyettes 2021-es londoni Kibervédelmi Kötelezettségvállalás Konferencián* elhangzott felszólalása szerint az elmúlt évben az új biztonsági fenyegetések, trendek megjelenése felgyorsult. Világszerte soha nem látott számú ember dolgozik, kommunikál, vásárol és szocializálódik otthonról. Képernyőkön keresztül a szemtől szemben kapcsolat helyett és interneten keresztül történik az információk megszerzése.

[115] NATO Comprehensive Cyber Defence Policy.

[116] Whole-of-government approach.

[117] The Secretary General's Annual Report 2021, „Comprehensive Approach to Cyber Defence" fejezet p. 30–31. o.

A kibertámadások száma növekszik, céljuk az emberek, a vállalkozók és végső soron a társadalmak; megpróbálják aláásni a demokratikus folyamatok és intézmények iránti bizalmat.

Fel kell készülni az ellenálló-képesség biztosítására és a gyors helyreállításra, bármilyen kibertámadásról is legyen szó.

A NATO-nak és minden szövetségesnek folytatnia kell az alkalmazkodást annak érdekében, hogy a digitális világban ugyanolyan legyen a biztonság és az ellenálló-képesség, mint a fizikai világban.

A Kibervédelmi Kötelezettségvállalás 2016-os elfogadása óta a szövetség hosszú utat tett meg.

A szövetségesek megállapodtak abban, hogy egy kibertámadás kiválthatja a kollektív védelmi záradék, az 5. cikk aktivizálását.

A kiberteret katonai műveleti területként azonosította a szövetség a szárazföld, a tenger, a levegő és az űr mellett.

A szövetségesek megállapodtak a nemzeti kiberhatások – más néven „offenzív kiber" – integrálásába a szövetség műveleteibe és misszióiba – növelve a válaszadási lehetőségeket.

A szövetség egy új Kibertérműveleti Központot alapított a helyzetismereti kép javítása és a jobb műveleti koordináció érdekében.

Együtt jobban kialakíthatók a kibertér globális szabályai és normái, illetve biztosítható, hogy azok megfeleljenek a szabadság, a demokrácia értékeinek és a jogállamiság követelményeinek.

A NATO ideális szerepet játszik a kibertér biztonságához szükséges szabályok, szabványok és normák kialakításához szükséges egyeztetésekhez, támogató folyamatokhoz, valamint az erőforrások összehangolásához annak érdekében, hogy e szabályokat betartsák.

A NATO Európában és Észak-Amerikában platformszerepet játszik a szövetségesek számára, hogy összehangolhassák a rosszindulatú kibertámadásokra adott válaszokat.

A szövetségesek nyilvánosan elítélik a destabilizáló és rosszindulatú kibertevékenységeket, és szorgalmazzák a nemzetközi jog és normák tiszteletben tartását, a felelős magatartást a kibertérben.[118]

2021-es esemény a NATO átfogó műveletttervezési irányelve legújabb változatának megjelenése, integrálva a kibertérműveleti kérdéseket is. A dokumentum a NATO stratégiai szintű tervezési feladatokat szabályozza, amivel egyértelmű iránymutatást

[118] Speech by NATO Deputy Secretary General at NATO Cyber Defence Pledge Conference 2021, London.

ad az alacsonyabb szintű feladatok tervezésére, beleértve a NATO–nemzeti feladattervezést is.[119]

A *NATO állam- és kormányfőinek 2022-es Brüsszeli Nyilatkozata* szerint a szövetségesek növelik a társadalom és az infrastruktúrák ellenálló-képességét Oroszország rosszindulatú befolyása ellen. Bővítik a kiberképességeket és -védelmet, támogatást nyújtanak egymásnak kibertámadás esetén.

A szövetségesek készek költségeket róni azokra, akik a kibertérben károkozásra törekednek, fokozzák az információcserét és a helyzetfelismerést, a civil felkészültséget, és erősítik a dezinformációra való reagálási képességet.[120]

A *2022-es madridi csúcsértekezlet* deklarációja szerint a szövetség kiber-, űr-, hibrid és egyéb aszimmetrikus fenyegetésekkel, valamint az új típusú és minőségugrást biztosító technológiák[121] rosszindulatú felhasználásával áll szemben. A szövetség rendszerszintű versenyben áll azokkal – köztük a Kínai Népköztársasággal –, akik kihívást jelentenek az érdekek, a biztonság és az értékek ellen, és a szabályokon alapuló nemzetközi rend aláásására törekszenek.

A szövetség új alapkövetelményeket[122] határoz meg az elrettentés és védelem érdekében.[123]

A NATO továbbra is megvédi a lakosságot, és mindenkor megvédi a szövetséges területek minden centiméterét. Építeni fog az újonnan kiterjesztett struktúrára, és jelentősen megerősíti az elrettentést és a védelmet, hogy hosszú távra szavatolja valamennyi szövetséges biztonságát és védelmét. Ez a 360 fokos megközelítéssel összhangban a szárazföldi, légi, tengeri, kiber- és űrterületeken minden fenyegetés és kihívás elleni védelmet jelenti.

Az ellenálló képesség nemzeti felelősség és kollektív elkötelezettség. A szövetségesek növelik ellenálló-képességüket, többek között nemzeti szinten kidolgozott célok és végrehajtási tervek révén, a közösen kidolgozott célkitűzések által vezérelve. Minden területen felgyorsítják az alkalmazkodást, növelve a kiber- és hibrid fenyegetésekkel szembeni ellenálló-képességet, erősítve interoperabilitást.

[119] Allied Command Operations: Comprehensive Operations Planning Directive (COPD, version 3.0).

[120] Statement by NATO Heads of State and Government, Brussels 24 March 2022.

[121] Emerging and disruptive technologies – EDT. A kifejezés magyar honosítása még nem történt meg. Tartalmilag az olyan megoldások felbukkanását jelenti, amelyek jelentősen felülírják a megjelenésük előtti eljárásokat, alapelveket (pl. a kvantumtechnológia fenyegetése a rejtjelző megoldások feltörésére, vagy önmagában a mesterséges intelligencia megjelenésének hatásai).

[122] Set a new baseline.

[123] A kibertérműveleteknél lényegesen magasabb szintű az a fogalmi megközelítés, hogy a korábbi stratégiamegfogalmazásokban olvasható „védelem és elrettentés" kifejezés 2022-ben „elrettenés és védelemmé" alakult. A jövőben látható lesz, hogy el a súlyponteltolódás milyen konkrét folyamatokat erősít vagy indít el a szövetségben. Most felelősségteljesen csak annyi jelenthető ki, hogy az eddigi trendeknek megfelelően ez a változás le fog csapódni a kibertérműveleti területre is, a stratégiai, hadműveleti és harcászati szintek szerint értelmezett folyamatokkal és képességekkel.

A szövetségesek integrált módon alkalmazzák a politikai és katonai eszközöket. A fokozott polgári-katonai együttműködés révén jelentősen megerősítik a kibervédelmet.

A szövetségesek önkéntes alapon és nemzeti eszközök felhasználásával úgy döntöttek, hogy virtuális gyorsreagálású kiberképességet[124] építenek ki és készítenek fel a jelentős hatású rosszindulatú kibertevékenységekre[125] történő reagálás érdekében.[126]

A *2022-es NATO Stratégiai Koncepció* megfogalmazása szerint a kibertérben folyamatos küzdelem van. Rosszindulatú szereplők arra törekszenek, hogy akadályozzák a kritikus infrastruktúrák működését, beavatkozzanak kormányzati szolgáltatásokba, hírszerzési információkat szerezzenek meg, szellemi tulajdont lopjanak el, és akadályozzák a katonai tevékenységeket.

A stratégiai versenykörnyezetben fokozni kell a globális tudatosságot; minden műveleti területen, irányban a 360 fokos megközelítéssel összhangban lévő elrettentést és védelmet kell kialakítani.

A NATO-szintű elrettentés és védelem kialakítása a nukleáris, a hagyományos és a rakétavédelmi képességek megfelelő összetételén alapul, amelyet űr- és kiberképességek egészítenek ki. Ez defenzív, arányos és teljes mértékben összhangban van nemzetközi kötelezettségvállalásokkal.

A katonai és nem katonai eszközök arányos, koherens és integrált módon kerülnek alkalmazásra minden biztonsági fenyegetésre történő reagálásként, saját választás szerinti módszerrel, időzítéssel és alkalmazási területen.

A szövetségesek tovább erősítik haderejük kollektív készenlétét, reagálóképességét, bevethetőségét, integrációját és interoperabilitását. Egyedileg és közösen biztosítják az elrettentéshez és a védelemhez szükséges erők, képességek, tervek, erőforrások, eszközök és infrastruktúra teljes skáláját, beleértve a nagy intenzitást is.

Erősítik a képzést és a gyakorlatokat, átalakítják és racionalizálják döntéshozatali folyamataikat, javítják tervezésüket és válságreagáló rendszerünk hatékonyságát.

A szövetség felgyorsítja a digitális átalakulást, hozzáigazítja a NATO-parancsnoki struktúrát az információs korhoz, és fejleszti a kibervédelmet, a hálózatokat és az infrastruktúrákat.

A hatékony elrettentés és védelem a kulcsa a világűr és a kibertér biztonságos használatának és a korlátlan hozzáférés biztosítása érdekében. A szövetség javítani fogja a képességeket, hogy hatékonyan működjön az űrben és a kibertérben a fenyegetések teljes spektrumának megelőzése, észlelése, leküzdése és az azokra való reagálás érdekében, minden rendelkezésre álló eszköz felhasználásával.

[124] Virtual rapid response cyber capability.

[125] Significant malicious cyber activities.

[126] Madrid Summit Declaration Issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Madrid 29 June 2022, 6, 9, 10.

Egyetlen művelet vagy halmozódó rosszindulatú kibertevékenységek, esetleg ellenséges műveletek az űrbe, az űrből vagy az űrben elérheti a fegyveres támadás szintjét, amikor az Észak-atlanti Tanács az Észak-atlanti Szerződés 5. cikkét lépteti érvénybe.

A szövetség elismeri nemzetközi jog alkalmazhatóságát, és előmozdítja a felelős magatartást a kibertérben és az űrben.[127]

A 2022-es római NATO Kibervédelmi Kötelezettségvállalás Konferencián a főtitkár megállapította, hogy Oroszország agressziójának része egy láthatatlan háború a kibertérben, amire példát jelentenek az orosz erők határátlépése előtti órákban és a későbbiekben is érzékelt kibertámadások.

A kiber állandóan vitatott tér. A béke, válság és konfliktus közötti határvonal elmosódott. Emiatt a NATO régóta komolyan veszi az állami és nem állami szereplők kibertérben érzékelhető fenyegetéseit.

A kiber(tér) ma már műveleti terület, egyenlően a szárazföldi, tengeri, légi és űrbeli műveletekkel. Több szövetséges felajánlotta nemzeti kiber hatásainak (cyber effects) használatát.

A NATO Kibervédelmi Kötelezettségvállalás következtében a szövetségesek növelték a kiberberuházásaikat, javították nemzeti stratégiáik végrehajtásához szükséges készségeiket és képességeiket.

A NATO rendszeres gyakorlatokat tart. Beleértve a NATO Cyber Coalition „zászlóshajó"-gyakorlatot, ami a világ legnagyobb gyakorlata.

A NATO egyedülálló platform, ahol a szövetségesek információkat osztanak meg, feltárják aggályaikat, megosztják egymással a bevált gyakorlatokat, és mérlegelik a kollektív válaszokat.

Szeptemberben az Észak-atlanti Tanács határozottan elítélte az Albánia nemzeti információs infrastruktúrája elleni közelmúltbeli kibertámadást, miközben a NATO személyzete Tiranába ment, és támogatást nyújtott. Albánia és más szövetségesek ezt a támadást Iránnak tulajdonították. Ez egy példa arra, hogy a NATO-szövetségesek összefognak, és egységesen válaszolnak.

A NATO szorosan együttműködik az EU-val kiberügyekben is. A szakértők (cyber defender) információkat osztanak meg a kiberfenyegetésekről, és részt vesznek egymás gyakorlatain, beleértve a NATO Cyber Coalition kibergyakorlatot is.

A NATO szorosan együttműködik partnerországokkal és magáncégekkel is, amelyek kulcsszerepet játszottak az ukrán kibertér védelmében. A Starlink műholdak biztonságos kommunikációt és internet-hozzáférést tesznek lehetővé. A Microsoft és az Amazon éppen akkor tudta feltölteni Ukrajna minisztériumait a felhőbe, amikor a szervereit az orosz lövedékek támadták. A YouTube és a közösségi média cégek blokkolták vagy korlátozták az orosz állami média- és trollfiókokat.

[127] NATO 2022 Strategic Concept; 15, 20, 22, 24 és 25.

A kormányok és a technológiai vállalatok közötti együttműködés lényegesen szorosabbá vált. Például a NATO és a Microsoft információkat cserél a szövetségesekre és Ukrajnára gyakorolt rosszindulatú támadások hatásainak mérséklésére

A júniusi madridi csúcson megállapodás történt, hogy továbbfejlesztjük az iparral való együttműködést, kiterjesztve azt az online szabványok és viselkedési normák kialakítására.

A kibertér nem lehet mindenki számára ingyenes „vadnyugat". Minden szövetséges egyetért abban, hogy az alapvető jogok és a nemzetközi jog éppúgy érvényesül online, mint offline.[128]

Szükség van a felelős használat elveinek kialakítására, amelyek tükrözik demokratikus értékeinket és emberi jogainkat.

1949-ben Truman elnök úgy jellemezte a NATO-t, mint „pajzsot az agresszió és az agressziótól való félelem ellen". Ma ez a pajzs a kibertérre is kiterjed.

„A kibertérből származó fenyegetés valós és növekszik, ezért fontos a Kibervédelmi Kötelezettségvállalás. Ezért felkérem a szövetségeseket, hogy kötelezzék el magukat a kibervédelem mellett, több befektetéssel, több szakértelemmel, megerősített együttműködéssel. Ez a kollektív védelmünk létfontosságú része."[129]

2022-es nemzeti esemény, hogy a NATO Kiberműveleti Doktrína kötelező jellegű érvényesülése mellett a Magyar Honvédség Parancsnoksága parancsnokának szakutasításaként[130] megjelent az MH Kibertér Műveleti Doktrína.[131]

Szervezetfejlesztési esemény, hogy az évben megalakult az MH Kiber és Információs Központ a korábban már szereplő Kiber Akadémia és egyéb meglévő szervezetek összevonásával.[132]

***

[128] … apply just as much online as they do offline.

[129] Keynote address by NATO Secretary General Jens Stoltenberg at the NATO Cyber Defence Pledge Conference in Italy (https://www.nato.int/cps/en/natohq/opinions_208925.htm).

[130] A szakutasítás jellegénél fogva – szervezetszabályozó közjogi eszközként – kötelező érvényű az MHP és alárendelt szervezetek esetében. Tartalmi kérdéseket tekintve az is nyilvánvaló, hogy a doktrína csak alapelvekkel, irányok meghatározásával ad segítséget az alkalmazó katonai szervezeti vezetőknek, konkrét feladatszabás helyett. Ez a kettősség aláhúzza a katonai vezetők képzésének szükségességét a viszonyrendszer helyes értelmezése és alkalmazása érdekében.

[131] 175/2022. (HK 4.) MH PK intézkedés a Magyar Honvédség Kibertér műveleti doktrína (1. kiadás) című szolgálati könyv kiadásáról. Megjelent a Magyar Honvédség Kibertér műveleti doktrínája (https://jogalappal.hu/megjelent-a-magyar-honvedseg-kiberter-muveleti-doktrinaja/).

[132] 32/2021. (VII. 23.) HM utasítás a Magyar Honvédség Kiber- és Információs Műveleti Központ kialakításával összefüggő egyes feladatokról.

1999-től kezdve a kezdeti kibertérműveletek általános megfogalmazásai, a fenyegetések említése mellett a NATO felső szintű megfogalmazásai egyre szélesebb körben, egyre több elemet tartalmaznak a kiberbiztonsággal, kibertérműveleti képességekkel kapcsolatban.

A fenyegetések súlyossága miatt a szövetség értékelése szerint már *nemzeti és szövetségi szintű stratégiai kockázatok kezelése szükséges.*

A fenyegetések súlyosságának említése és az ezek ellensúlyozására szolgáló védelem mellett *egyértelműen azonosítható az integrált megközelítés gondolata*, ahol a kibertér nem önállóan jelenik meg – kiemelt elemként –, hanem a többi műveleti terület között foglalja el helyét, integráns részét képezi az összhaderőnemi[133] műveleteknek. Ez egyben „átjárhatóságot" is jelent, azaz kibertérműveletek ellen válasz lehet kibertérműveleti vagy fizikai jellegű, illetve fizikai jellegű műveleteket is támogathat kibertérművelet. A fantasztikus filmek szintjét elérő „kibertérművelet kibertérművelet ellen" speciális eset az előbbiek mellett szintén elképzelhető, de ez napjainkban még nem képez elsődleges megoldást – de nem jósolható meg, hogy mikor kerül sor az első ilyen konfliktusra.

Az áttekintett források *többszörösen megfogalmazzák a kibervédelem, kibertérműveletek vonalán a hírszerzési információk integrálásának szükségességét a szövetségi folyamatokba.* A NATO-nak és szövetségeseknek egyaránt létfontosságú a hírszerzési funkciók kibertérben történő megvalósítása.

A NATO védelmi jellegének hangsúlyozása mellett egyértelmű, hogy a szövetség nem mond le a katonai műveleteket támogató kibertérműveletek alkalmazási lehetőségéről, beleértve az offenzív hatásokat (offensive effects) is, ami jelenleg nemzeti végrehajtásban elképzelt.

Kezdetben a NATO-hálózatok biztonságának növelését célzó hálózatfejlesztési kérdések és ehhez tartozóan az eseménykezelés centralizált kezeléséhez szükséges szervezetépítés és képességfejlesztés volt fókuszban. Ezt a vonalat erősítve megjelentek a védelempolitikai, stratégiai együttműködési feladatokat szolgáló szervezeti elemek, illetve a szövetségesekkel történő közös platformot biztosító keretek (Policy, Strategy). Ennek a sornak legutolsó eleme a NATO Kibertérműveleti Központ megalakítása Monsban, ami a NATO-hálózatok eseménykezelési feladatai mellett a katonai műveletekbe történő integrálást célzó lépés.

Nem felejthető, hogy *az elektronikus szolgáltatások, hálózatok biztonságának alapvető pillére az üzemeltetési és az infomációvédelmi (benne elektronikus információvédelmi)*[134] *követelmények sikeres teljesítése.*

[133] Az aktuális megközelítés szerint az „összhaderőnemi" megfogalmazás helyett például hatásalapú, átfogó megközelítésű, multi domain műveletek.

[134] A magyar jogszabályok minősített adatkezelés esetén az „elektronikus információvédelem", nem minősített adatok kezelése esetén az „elektronikus információbiztonság" kifejezést alkalmazzák. Ezt az elkülönítést a NATO nem alkalmazza.

Több mint tíz évvel ezelőtt *megkezdődött a szövetségesek és a NATO eseménykezelését, bevált gyakorlatok cseréjét és egyéb kapcsolattartási célokat szolgáló együttműködési megállapodások rendjének kialakulása*, ami 2016-ban már második fejlettségi fázisba lépett. Az EU eseménykezelő szervezet is csatlakozott ehhez az együttműködési rendhez, illetve 2016-ban legmagasabb szintű együttműködési megállapodás született a NATO és az EU között.

A szövetség hosszú évek óta következetes, egyértelmű megfogalmazást ad *a nemzetközi normák alkalmazásával kapcsolatos elkötelezettségéről,* illetve fontos kérdésként kezeli a helyes állami viselkedési normák önkéntes alapú kialakítását.

Több mint tízéves múltja van a szövetségi kibervédelmi gyakorlatoknak, a NATO-gyakorlatokba történő kiber-forgatókönyvek bedolgozásának, illetve kialakult ez a gyakoroltatási lehetőség a NATO Kibervédelmi Kiválósági Központ szervezésében is. Az észt tulajdonú és üzemeltetésű Cyber Range mindkét rendezvénytípus kiszolgálását végzi.

Képzés területén a NATO kiképzőközpontok által biztosított lehetőség mellett a NATO Kibervédelmi Kiválósági Központ biztosít technikai, jogi, hadműveleti alkalmazási és egyéb szaktanfolyamakat, ami jelzi a szakterületüket.

A NATO műveletтervezési eljárásrendben részletesen megjelentek a kibertérműveleti kérdések, illetve a magasabb szintű doktrínák általános irányelvei mellett megjelent a NATO Kibertérműveleti Doktrína is a műveletek végrehajtása során szükséges szakmai támogatás érdekében.

A katonai kibertérműveleti alkalmazásra vonatkozó NATO stratégiai szintű vizsgálat tudatosan szűkített célt jelent, de a 2010-es évek közepétől *jól felismerhető az ellenálló-képesség és a hibrid műveletek témakörök egyre erősödő, tartalmilag szélesedő megjelenése.* Emiatt – és *az elrettentés fogalmának helyes megközelítése érdekében* – szükséges annak rögzítése, hogy a kibertérműveletek védelempolitikai, stratégiai szintű értelmezése kizárólag e *három fogalmi kör figyelembevételével történhet.*

SPITZER JENŐ – VIKMAN LÁSZLÓ

Katonai és Nemzetbiztonsági képességfejlesztések és azok jogi, jogpolitikai háttere egyes transzatlanti államokban

1. KÉPESSÉGFEJLESZTÉSI TÖREKVÉSEK ÉS AZOK NEMZETKÖZI KERETEI

Európa biztonsági realitása mára a háborús környezet, úgy, hogy közben az ezredfordulón globálissá és kiterjedtté vált terrorizmus, az államműködést is befolyásolni tudó szervezett bűnözés, az időnként erőszakossá fajuló társadalmi feszültségek sem szűntek meg. Több, a második világháborút követően, a hidegháború időszakában kifejlesztett és egyes komponenseit tekintve a nagyhatalmak közti proxyháborúkban bevetett, így kipróbált védelmi-biztonsági szervezet, eljárásrend és fegyverrendszer generációváltása elodázhatatlanná vált a múlt század 90-es éveinek békeeufóriájából sokkszerűen ébredő országokban.

A Stockholmi Nemzetközi Béke Kutatóintézet (SIPRI) 2022-es évkönyve[1] szerint a globális fegyverkezési költések már hetedik éve folyamatosan nőnek, világszinten 2113 milliárd USD-t tesznek ki, ezzel az összes ország GDP-jének 2,2%-át kitéve, hozzátéve, hogy ezzel egy időben a teljes kormányzati költések nagyobb ütemben növekedtek. Európában az előző évhez képest mért növekedés még nagyobb volt, elérte a 3%-ot. A globális fegyverkereskedelem 77%-án exportőrként csupán öt ország osztozik: USA, Oroszország, Franciaország, Kína és Németország. A teljes fegyverimport 13%-a jutott Európára 2017–2021 közt, és a 2012–2016-os időintervallumhoz képest 2017–2021 közt ez a volumen 19%-kal nőtt. Ezek az adatok egyértelműen visszajelzik a kontinensünkön romló biztonsági helyzetet.

A hazánkat is érintő szövetségi kereteket vizsgálva az EU esetében[2] az elmúlt időszak legfontosabb eseményei között elsőként talán a 2016-ban elfogadott új globális kül- és biztonságpolitikai stratégiát[3] hozhatjuk fel. Az ezt követően, 2017 vé-

[1] *Sipri Yearbook 2022 – Armaments, Disarmament and International Security*. 12, 15. o. (https://www.sipri.org/yearbook/2022).

[2] B. Müller Tamás: Európai Uniós védelmi kezdeményezések és a PESCO. *Infojegyzet*, 2020/90. szám.

[3] Shared Vision, Common Action: A Stronger Europe. The strategy document 'A Global Strategy for the European Union's Foreign and Security Policy. 2016. (https://www.eeas.europa.eu/eeas/global-strategy-european-unions-foreign-and-security-policy_en).

gén elindított Állandó Strukturált Együttműködés (PESCO)[4] arra ösztönözte az önkéntes alapon együttműködő tagállamokat, hogy magasabb szintű védelmi kötelezettségvállalásokat tegyenek, és új képességfejlesztési projekteket indítsanak. Az EU 2018-as Képességfejlesztési Terve (CDP)[5] egyrészt a tagállamok nemzeti védelmi tervezését támogatja, másrészt az EU védelmi eszközrendszerének legfontosabb referenciájaként szolgál. 2020-ban először készült el a Koordinált Éves Védelmi Felülvizsgálat (CARD),[6] melynek célja az volt, hogy uniós szinten áttekinthetőbbek legyenek a védelmi kiadások, a nemzeti beruházások és a védelmi vonatkozású kutatási tevékenységek. Az Európai Védelmi Alapot (EDF) pedig arra hozták létre, hogy a nagyrészt az együttműködéseken alapuló képességfejlesztési programokat finanszírozza, kiemelt figyelmet fordítva a védelmi ipar és innováció támogatására. Lényeges, hogy az alapból egy meghatározott határig a PESCO projektek is részesülhetnek, és hogy az alap létrehozásával az EU először költött a közös költségvetésből haderőfejlesztésekre, ezzel is erősítve a közösségi biztonság- és védelempolitikai törekvéseket.

Az Észak-atlanti Szövetség, mint alapvetően az ENSZ Alapokmánya szerint a kollektív védelemre létrejött katonai szövetség a kezdetektől fontos szempontként kezeli a haditechnikai innovációt és fejlesztést, a haderő-transzformációt.[7] A 2014-es walesi csúcstalálkozó záródokumentumában[8] a tagállamok megállapodtak az éves GDP 2%-át elérő védelmi büdzsészint fokozatos elérésében, és abban is, hogy a költéseik 20%-a legalább új fejlesztések fedezete lesz. Ezt a szintet a 2018-as brüsszeli záródokumentumban[9] már úgy becsülték, hogy 2024-re 24 tagállam fogja elérni. A kiberterület szempontjából lényeges fejlemény volt a 2016-os varsói csúcson elfogadott Cyber Defence Pledge[10], és általában is a technológiai fejlődést meszszemenően figyelembe vevő Warfighting Capstone Concept[11] kiadása 2021-ben. A szintén 2021-es NATO 2030 jelentést[12] követően 2022-ben – a várható finn és svéd csatlakozás mellett – a legfontosabb fejlemény a madridi csúcson elfogadott új Strategic Concept dokumentum volt, ami képességfejlesztés témájában teljes mér-

[4] A PESCO weboldala: https://www.pesco.europa.eu/.

[5] European Defence Agency Capability Development Plan (CDP).

[6] 2020 CARD Report: https://eda.europa.eu/docs/default-source/reports/card-2020-executive-summary-report.pdf.

[7] Lásd a 2003-ban létrehozott NATO Szövetségi Transzformációs Parancsnokság tevékenységét (https://www.act.nato.int/).

[8] NATO Wales Summit Declaration.

[9] NATO Brussels Summit Declaration.

[10] NATO Cyber Defence Pledge.

[11] John W. Tammen: NATO's Warfighting Capstone Concept: anticipating the changing character of war. *NATO Review*. 2021. (https://www.nato.int/docu/review/articles/2021/07/09/natos-warfighting-capstone-concept-anticipating-the-changing-character-of-war/index.html).)

[12] Lásd Siposné Kecskeméthy Klára: A NATO 2030 jelentés – stratégiai prioritások új megközelítésben. *Honvédségi Szemle*, 2021/4. szám, 3–16. o.

tékig elkötelezett, kiemelve az űr és kiberképességeket, és célként fogalmazza meg a szövetségesek képességeinek még erősebb integrációját.

A harceszközök tényleges értékét vagy a kifejlesztésükre fordított források hasznosulását mindig a gyakorlati alkalmazás árazza be pontosan (az adott szituációban), és a tömegmédia eszközeivel végigkövetett konfliktusok kínosan hamar rámutatnak egyes fegyverrendszerek evolúciós zsákutcáira vagy az elmulasztott és halogatott fejlesztések „költségeire". Mindezzel együtt a siker és kudarc közt nem kizárólag egy fegyverrendszer fejlettsége, robusztussága, sokoldalúsága és hatékonysága dönt, legalább ekkora hangsúlyt kap a kiképzett és szakértő kezelőszemélyzet, a támogató logisztikai ellátás, és a megfelelő vezetés-tervezés mellett az integráltság is az adott állam fegyveres erejébe – jogász szemmel nézve akár a harcszabályzatoktól a doktrinális háttéren át egészen a jogszabályok szintjéig terjedő szabályozási háttér meglétével. Az államok védelmi képességeinek fejlesztésében jelenleg technológiai, jogi és költségvetési kötöttségek mellett a globális ellátási lánc zavarai, a hirtelen megnövekedett kereslet és a hiányzó védelmi ipari infrastruktúrák is azt eredményezik, hogy nem lehetséges egy pillantás alatt egy minden háborút megnyerő, de legalábbis az állam saját súlyához mérten ütőképes hadsereg előteremtése.

Az IKT-technológiák rohamos fejlődése miatt sok olyan új eszköz is megérkezett már a gyártóktól rendszeresített eszközként a fegyveres erőkhöz,[13] mi több a harcmezőkre, amelyekre vonatkozóan a nemzetközi jog nem (sőt néha még a nemzeti sem) rendelkezik egyértelmű útmutatással az elfogadható és humanitárius jognak megfelelő alkalmazásra, de teljes mértékben az átfogó védelmi-biztonsági szisztémába való integrálásra sem. A nemzetközi egyezményekkel már „lefedett" képességek esetében sem mindig egyértelmű a jogértelmezés egy fegyveres konfliktusban, de még inkább igaz ez az új, diszruptív és várhatóan nagy hatással bíró eszközök és fejlesztések vonatkozásában, mivel ezek biztonságpolitikai, hadászati, etikai és jogi megítélése sem kristályosodott ki még. Ez annál is inkább sürgős feladat lenne, mivel a szóban forgó technológiák és felhasználási módjuk (mesterséges intelligencia, kiberhadviselési eszközök, drónok és autonóm fegyverrendszerek, a kibertérben folytatott információs hadviselés stb.) aránylag kisebb ráfordítással, de célzottan nagy hatás elérésére alkalmasak a kritikus infrastruktúrákat vagy közvetlenül a lakosságot érintve.

Ezek az új technológiák minden jelenlegi haderőfejlesztési programban szerepelnek a beszerzendő eszközök listáján, de a már említett kérdésekre még nem születtek meg a megnyugtató válaszok. Ebben a tanulmányban arra teszünk kísérletet, hogy – idősíkban a 2014-es krími orosz agressziótól és a NATO walesi csúcsértekezletétől a NATO 2022-es madridi csúcsáig – néhány meghatározó állam képességfejlesztési lépéseit és a hozzájuk kapcsolódó biztonságpolitikai, etikai, jogi diskurzust

[13] Vö. Porkoláb Imre – Hennel Sándor – Hegedűs Ernő: Modernizáció és innováció (1.). *Honvédségi Szemle*, 2021/2. szám, 14–26. o.

röviden bemutassuk, majd adjunk egy rövid betekintést abba is, hogy melyek azok a védelmi ipari innovációs irányok, amelyek várhatóan még további feladatokat fognak generálni, mely eszközök alkalmazása, bevezetése hozhat magával védelempolitikai, etikai és jogi problémákat.

A képességfejlesztés tágan értelmezve több irányból is megközelíthető, komplex tevékenység: az elsősorban mérnöki-technikai-harcászati szemlélet[14] mellett lehetséges azt szervezeti vagy szabályozási oldalról is értékelni,[15] ami például a döntéshozatal műveleti tempónak megfelelő biztosításával, rugalmasságával és a szakmai szint részére megfelelő mozgástér biztosításával sokat tehet a tényleges képesség teljes kihasználásáért. Fakadóan a szerzők szakterületéből is, ezért a technikai újítások mellett inkább nagyobb figyelmet igyekeztünk fordítani az egyes államok újszerű, az adott eszközrendszerhez igazítva kialakított szervezeti megoldásaira. Ezt az a jelen kötetben is hangsúlyozott komplex hatásmátrix is alátámasztja, amely az infokommunikációs fejlesztések sokrétű társadalmi-politikai, illetve jogi-államszervezési kihívásaira mutat rá.

Mindezek mellett azért, hogy valamiféle objektív összemérhetőséget, súlyozást is fel lehessen mutatni a vizsgált országok vonatkozásában – akár olyan megközelítéssel is, hogy ki mire költ, milyen területeket tart fontosnak, milyen új képességektől várnak előrelépést –, feltüntetjük a Global Firepower Index által számított 2022-es értéket is[16] (tájékozódási pontként ez hazánk esetében 0.8633, ami az 57. helyezéshez elegendő).

2. JOGI KÉRDÉSEKET FELVETŐ KÉPESSÉGFEJLESZTÉSEK EGYES TRANSZATLANTI ÁLLAMOKBAN

2.1. Egyesült Államok (PwrIndx: 0.0453, 1. helyezés)

A 20. századot a domináns világpolitikai gazdasági és katonai hatalomként záró USA hegemón szerepe egyre inkább megkérdőjeleződik, az unilaterális világ és a második világháborút lezáró nemzetközi egyezmények által meghatározott világ-

[14] Lásd pl.: Pölöskei János: A képességalapú haderőtervezés. *Honvédségi Szemle*, 2021/6. szám, 36–46. o.

[15] Lásd pl.: Gazdag Erika: Koncepciófejlesztés a NATO-ban. *Honvédségi Szemle*, 2022/3. szám, 3–19. o.

[16] Ezt az indexet több mint 50 különböző faktorból (katonai képességek, pénzügyi és logisztikai háttér, földrajzi adottságok stb.) számítják, ez adja az adott ország katonai erőindexét (PwrIndx). A képlet belső súlyozása összevethetővé teszi a méretekben eltérő országok összevetését is, azzal, hogy a nukleáris képességeket nem tették a képlet részévé. Az index értéke minél alacsonyabb, annál nagyobb erőt jelez, a 0,0 érték nem érhető el. Részletesebben lásd: https://www.globalfirepower.com/countries-listing.php (Elérés dátuma: 2022. november 14.).

rend (rules based order – az angol szakirodalomban) egyre inkább egy multipoláris felállás felé mozog, ahogy az erősödő, és erejét projektálni is kívánó Kína a csendes-óceáni régióban színre lép, és más, inkább regionális hatalmak is igyekeznek a saját érdekszférájuk határait kitolni. Az USA katonai erejét hiba lenne az iraki és afganisztáni hadszíntérről történő, és kérdéses eredményeket felmutató hadjáratait követően kétségbe vonni, de tény, hogy sok kisebb regionális szereplőt, és az ezekből a konfliktusokból sokat tanuló nagyobb aktorokat is felbátoríthatták ezek a kudarcok.

A világ legnagyobb hadiiparával, a legkorszerűbb technológiával felszerelt fegyveres erőivel rendelkező ország esetében lehetetlen küldetés lenne egyes képességekre felhívni a figyelmet, és valószínűleg kétes értéke is lenne, hiszen hazánk esetében nem sok jelentősége van a Ford anyahajó képességeinek, és nagyobb mennyiségben az ötödik generációs F-35-ös is valószínűleg drága lenne a magyar költségvetés számára.[17] Érdemesebb néhány olyan elemzésre és új szervezeti megoldásra koncentrálni, amelyek a folyamatos innovatív és adaptív képességfejlesztést és a diszruptív technológiák utáni kutatást erősíthetik, mivel ezek más országok számára is példaként szolgálhatnak.

1947-ben alakították meg az USA-ban a légierőt (US Air Force), azóta a haderőnemi felosztás gyakorlatilag változatlan volt (Army – szárazföldi erők, Navy – haditengerészet, Marines – tengerészgyalogság és Coast Guard – parti őrség).[18] 2019 decemberében törvénybe iktatták, majd 2020 januárjában első parancsnokát is megkapta a Space Force mint új szervezet. Parancsnokát, állományát, bázisait, technikai eszközeit legnagyobbrészt a légierőtől kapta, de érkeztek szakemberek, erőforrások és eszközök más haderőnemektől is, amelyek korábban a világűr saját szempontú, haderőnemi aspektusai miatt már máshol működtek. Ezzel létrejött a fegyveres erők 6. ága (branch), amelybe csak az Air Force-tól 16 000 ember érkezett. Feladatai[19] közül egyelőre a leginkább az egyes eszközök űrbe juttatása, a Védelmi Minisztérium, a NASA és kereskedelmi űrvállalkozások repülésbiztonságának felügyelete, a Védelmi Minisztérium műholdjainak és eszközeinek az üzemeltetése, és segítségükkel a többi fegyveres erő támogatása a fontos. Egyértelmű törekvés azonban, hogy a Space Force képességein keresztül minél előbb hatékony és domináns

[17] Bár például Lengyelország Európa egyik legerősebb hadseregét kívánja kiállítani, válaszul az ukrán–orosz háború által is jelzett új biztonsági kihívásokra, amelynek részeként ebből a vadászgéptípusból is vásárolni szeretne, 500 HIMARS rakétavetővel, M1A2 harckocsikkal, Patriot-ütegekkel egyetemben. Részletesen lásd pl. Bartosz Głowacki: Poland moves to buy HIMARS, capping major May modernization push. *Breaking Defense.* 2022 (https://breakingdefense.com/2022/06/poland-moves-to-buy-himars-capping-major-may-modernization-push/).

[18] United States Spaces Force Summary 2019 February: (https://media.defense.gov/2019/Mar/01/2002095012/-1/-1/1/UNITED-STATES-SPACE-FORCE-STRATEGIC-OVERVIEW.PDF).

[19] About the United States Space Force (https://www.spaceforce.mil/About-Us/About-Space-Force/).

legyen az űrdomainben, és mind taktikai jellegű válaszok adására,[20] mind klasszikus értelemben véve harc megvívására is képes legyen.[21]

Önmagában természetesen egy ilyen átszervezés jelenthetne egyszerű fókuszáthelyezést, ami leköveti a műholdakon alapuló navigáció, infokommunikáció és szenzoros technológiák jelentőségének és lehetőségeinek masszív növekedését. Vélhetnénk akár azt is, hogy a meglévő nemzetközi jogi környezet bizonyos értelemben a még inkább nemzetközi jogilag elismert tilalomfákat nélkülöző kibertéri joghoz képest előrébb tart, hiszen ott van például a Magyarország által is ratifikált *Szerződés az államok tevékenységét szabályozó elvekről a világűr kutatása és felhasználása terén, beleértve a Holdat és más égitesteket*[22]. Ennek IV. cikke kimondja: „A Szerződésben részes államok kötelezik magukat, hogy nukleáris fegyvereket vagy bármely másfajta tömegpusztító fegyvert hordozó semmilyen objektumot nem juttatnak föld körüli pályára, ilyen fegyvereket az égitesteken nem helyeznek el, illetve a világűrben semmilyen más módon sem tartanak. A Holdat és más égitesteket a Szerződésben részes összes államok kizárólag békés célokra használhatják. Az égitesteken katonai támaszpontokat, berendezéseket és erődítéseket létesíteni, bármilyen fajta fegyverekkel kísérletezni és katonai gyakorlatokat folytatni tilos. Katonai személyeknek tudományos kutatásra vagy bármely más békés célra történő alkalmazása nincs tiltva. A Hold és más égitestek békés kutatásához szükséges bármely felszerelés vagy eszköz használata szintén megengedhető."

Nem tűnik véletlennek, hogy a (lassan majd klasszikusnak vagy elsőnek nevezett) hidegháború végén, Reagan elnök által indított „csillagháborús" program[23] is a világűrbe vitte a Szovjetunióval folytatott fegyverkezési versenyt, és most – a már említett technikai-gazdasági okok mellett – a multipolaritás ismételt megjelenésével ismét felmerül ez a domain is, mint a kompetíció egy színtere. Tudható, hogy az USA mellett több ország (Oroszország, Kína, India, feltevések szerint Izrael) rendelkezik például műholdak megsemmisítésére alkalmas technológiákkal,[24] és feltehető, hogy az űrdomainben lévő eszközök is egyre kifinomultabbak lesznek, ezzel együtt jogi szempontból is egyre több kérdést vetnek fel majd. Nem véletlen, hogy ezzel a területtel egyre kiterjedtebb – egyébként a kibertémát feldolgozó Tal-

[20] US Space Force Developing Plans (https://www.c4isrnet.com/battlefield-tech/space/2022/04/20/us-space-force-developing-plans-for-tactically-responsive-capabilities/).

[21] David Vergun: Partnerships Key to Space Force Delivering Warfighting Capabilities. *US DoD News.* 2021 (https://www.defense.gov/News/News-Stories/Article/Article/2471770/partnerships-key-to-space-force-delivering-warfighting-capabilities/).

[22] A „Szerződés az államok tevékenységét szabályozó elvekről a világűr kutatása és felhasználása terén, beleértve a Holdat és más égitesteket" című, Moszkvában, Londonban és Washingtonban 1967. január 27-én aláírt szerződés kihirdetéséről szóló 1967. évi 41. törvényerejű rendelet.

[23] Lesley Kennedy: Why Reagan's ‚Star Wars' Defense Plan Remained Science Fiction. *History.* 2019. (https://www.history.com/news/reagan-star-wars-sdi-missile-defense).

[24] Kyle Mizokami: Anti-Satellite Weapons Are Becoming a Very Real Threat. *Popular Mechanics.* 2020 (https://www.popularmechanics.com/military/weapons/a32008306/anti-satellite-weapons/).

linn kézikönyvet példaként véve –, de egyelőre inkább leíró jelleggel foglalkozó jogi kézikönyvprojektek is vannak már.[25] Az űrrel mint műveleti térrel természetesen a NATO szakértői is egyre behatóbban foglalkoznak,[26] ezért várhatóan a magyar katonai és hadijogi szakértők sem maradhatnak le sokkal a fősodortól.

A képességfejlesztés szervezeti oldaláról érkező megoldás az Army berkein belül 2018 nyarán aktiválásra került, kifejezetten jövőfókuszú Army Futures Command[27] is. 2019 júliusára teljes műveleti képességgel működött, és 2022 már 30 Mrd USD költségvetéssel látott neki a kitűzött modernizációs prioritásoknak. 2019-ben már 24 000 ember tartozott ide, ami természetesen annak volt köszönhető, hogy a korábban több parancsnokság alatt lévő K+F+I laboratóriumokat, intézeteket az új szervezeti ernyő alá koncentrálták. Munkafilozófiájában erősen épít a vállalkozásokkal, oktatási intézményekkel kiépített szoros szakmai kapcsolatokra, közös projektekre. Konkrét fejlesztéseken túl fenyegetettségértékeléssel, trendelemzéssel, koncepciók kidolgozásával, egészségügyi kutatásokkal is foglalkozik. Az Austinba telepített Army Software Factory részlegfeladat pedig egy olyan integrált szoftverfejlesztő kezdeményezés működtetése, amelyben vegyesen civil és egyenruhás hallgatók tanulhatnak, dolgozhatnak, és olyan alkalmazásokat készíthetnek, amelyek reményhetőleg segítenek a jelenlegi és jövőbeli képesség versenyképessé formálásához.

Érdemes röviden megvizsgálni, hogy egyébként a csúcstechnológiai fejlesztésekben élenjáró USA mely vívmányokat, találmányokat tekinti igazán jelentősnek, képesnek arra, hogy alkalmazásukkal kritikus előnyhöz juttassa az azt bevető felet, egyszerűbben, melyek a diszruptív (katonai) technológiák. Egy az amerikai Kongresszus számára készített tájékoztató[28] anyag hat ilyen területet emel ki:

- mesterséges intelligencia
- halált okozó autonóm fegyverrendszerek
- hiperszónikus fegyverek (a légvédelem szempontjából nem vagy nagyon nehezen elháríthatók)
- irányított energiafegyverek (új lézertechnológiák)
- biotechnológia
- kvantumtechnológia (a jelenlegi kriptográfiai technológiák azonnali elavulttá tételét jelentheti a gyakorlati alkalmazása mind a dekódolás, mind a titkosítás oldaláról)

[25] A két legfontosabb a MILAMOS (https://www.mcgill.ca/milamos/) és a Woomera (https://law.adelaide.edu.au/woomera/).

[26] Lásd. NATO Legal Gazett #42 December 21, Legal Aspects of Space: NATO Perspectives (https://www.act.nato.int/application/files/5716/4032/2170/legal_gazette_42.pdf).

[27] Army Futures Command (https://armyfuturescommand.com/).

[28] Emerging Military Technologies: Background and Issues for Congress. 2022. (https://sgp.fas.org/crs/natsec/R46458.pdf).

Természetesen több megközelítés[29] is létezik az ilyen listák összeállítására, azonban az már a fentiekből is jól érzékelhető, hogy a 21. század új fegyverrendszerei képességeikben messze túlmutatnak azokon, amelyekre vonatkozóan a nemzetközi jog a hágai és genfi egyezményekben valamilyen szintű szabályozást alkotott. Az emberi beavatkozástól független, mi több, az emberi közrehatást egyszerűen a reakcióidő rövidsége miatt szinte kizáró működés, vagy a biotechnológia esetében az előre nem látott következmények kockázatai egyre súlyosabb jogi, de morális kérdéseket[30] is felvetnek majd, amelyekre még nem feltétlenül rendelkezünk válaszokkal.

A mesterséges intelligencia vonatkozásában Brian Katz leszögezi,[31] hogy az erre építő megoldások képesek lehetnek a nemzetbiztonsági szféra működésének átformálására és erősítésére, de ez érvényes az ellenérdekelt felek oldaláról ugyanígy. Ezek az eszközök segíthetnek az adatfeldolgozás kiszélesítésében, automatizálásában és relevanciájának növelésében, ezzel hatékony támogatást jelentve az elemzői munkához, ami a döntéshozói tevékenységet segítheti időszerű, testreszabott információkkal. Az USA-nak azonban nemcsak a külső ellenfelekkel szemben kell megnyernie ezt a versenyt, hanem saját belső bürokratikus, technikai és szervezeti akadályait is el kell hárítania a cél érdekében.

A RAND Corporation egyik elemzéséből[32] pedig azt emelnénk ki, hogy az amerikai hírszerző közösség tevékenységét kiértékelve arra jutottak, hatékonyabb 21. századi hírszerző munkához egyrészt érdemes lenne egy dedikáltan nyílt forrásokkal dolgozó (gyűjtő/feldolgozó) új szervezet létrehozása, másrészt érdemes lenne megfontolni a hírszerzési eredmények szolgáltatásként elérhetővé tételét az amerikai nyilvánosság számára. Ha megfontoljuk, elméletileg egyik felvetés sem elképzelhetetlen, hiszen minden értékelő-elemző tevékenység erősen épít nyílt forrásokra is, és például mindenkinél ott lévő, egész jó minőségű mobilkészülékek, a közösségi platformok, a szinte mindenhol jelen lévő és weben keresztül is elérhető kamerák kimeríthetetlen információforrások, sőt éppen a túl nagy mennyiségű adat jelenti már a problémát. Úgyszintén nem ismeretlen dolog az állam és a nemzeti szempontok szerint stratégiai jelentőségűnek tekintett vállalatok együttműködése (lásd például a HUAWEI és Kína helyzetét), más kérdés, hogy a konkrét megvalósítást

[29] További példaként lásd: Critical and emerging technologies list update, (https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf).

[30] C. Anthoni Pfaff: The Ethics of Acquiring Disruptive Military Technologies. *Texas National Security Review,* 2019/2020 Winter (https://tnsr.org/2020/01/the-ethics-of-acquiring-disruptive-military-technologies/).

[31] The Intelligence Edge: Opportunities and Challenges from Emerging Technologies for U.S. Intelligence CSIS Briefs. 2020 (https://www.csis.org/analysis/intelligence-edge-opportunities-and-challenges-emerging-technologies-us-intelligence).

[32] Cortney Weinbaum – Bradley Knopp – Kim Soo – Yuliya Shokh: Options for Strengthening All-Source Intelligence. *Rand Corporation Research Report.* 2021 (https://www.rand.org/pubs/research_reports/RRA1245-1.html).

alaposan előre kidolgozott szabályokkal lehet csak elképzelni, különösen a források és eszközök védelme, a betekintés mélysége, a titoktartás és mindennek ellenőrzése vonatkozásában, hiszen mindezek nélkül az alaptevékenység sérülhet.

2.2 Franciaország (PwrIndx: 0.1283, 7. helyezés)

Franciaország (ahogyan azt a tanulmány során zsinórmértékként használt Global Firepower Index értéke is alátámasztja) jelenleg Nyugat-Európa egyik legnagyobb mértékben kapacitált hadseregével rendelkezik, ami annak köszönhető, hogy az ország elkötelezett a nemzeti katonai képességek minél szélesebb skálájának fenntartása mellett, és megőrizte képességét arra, hogy szövetségesek nélkül is képes legyen konfliktusok kezelésére, beleértve akár egy nagy intenzitású reguláris háborút is. Ezek a védelmi felfogások jelentősen kiegészültek az ország növekvő nemzetközi katonai szerepvállalásaival.[33]

Franciaországnak a nemzeti védelemről és biztonságról készült stratégiáját tartalmazó alapdokumentuma, a Fehér Könyv[34], valamint a kapcsolódó beszerzések és fejlesztések mentén[35] az ország legfontosabb stratégiai aspektusai a következőkben állapíthatók meg:

1. Franciaország atomhatalom, és ebbéli státuszának fenntartása alapvető cél;
2. Franciaországnak képesnek kell lennie arra, hogy bármikor és bárhol beavatkozzon nemzeti érdekeinek védelme érdekében; valamint
3. a francia védelmi ipar mindenkor védendő nemzeti érdek.

Franciaország a 2019–2025 időszakra tervezett védelmi fejlesztési programjában[36] már növelte védelmi kiadásait: megerősítette elkötelezettségét a NATO azon céljának elérése mellett, hogy bruttó hazai termékének 2%-át költse védelemre, továbbá

[33] Ezek kapcsán lásd: Discours du Président Emmanuel Macron sur la Stratégie de Défense et de Dissuasion Devant les Stagiaires de la 27ème Promotion de l'École de Guerre. *Elysée*, 2020. február 7. (https://tinyurl.com/bd45a9j2); Sondage: 75% des Français Soutiennent l'Intervention au Mali. *Le Parisien*, 2020. (http://www.leparisien.fr/international/sondage-75-de-francais-soutiennent-lintervention-au-mali-15-01-2013-2483685.php).

[34] Livre blanc de la défense et de la sécurité nationale (Fehér Könyv a nemzeti védelemről és biztonságról). (http://www.livreblancdefenseetsecurite.gouv.fr/pdf/le_livre_blanc_de_la_defense_2013.pdf).

[35] Példaként lásd Boris Toucas: *Understanding the Implications of France's Strategic Review on Defense and National Security.* Center for Strategic and International Studies, 2017; Nicolas Roche: Pourquoi la Dissuasion, Paris: Presses Universitaires de France. 2017; Corentin Brustlein: Forces Nucléaires Françaises, Quel Renouvellement? *Politique Étrangère*, 2017/3. szám.

[36] La loi de programmation militaire 2019–2025 et les capacités des armées (LPM). Ennek kapcsán lásd: La loi de programmation militaire 2019–2025 et les capacités des armées. Cour des Comptes. 2022 (https://www.ccomptes.fr/fr/publications/la-loi-de-programmation-militaire-2019-2025-et-les-capacites-des-armees).

kiemeltem hangsúlyt fektetett a koalíciós műveletekre. Fontos azonban megjegyezni, hogy Franciaország nézetei a NATO-szövetségesi tehermegosztásról eltérnek az Egyesült Államokétól: a franciák a hadseregük aktív tengerentúli műveleteit – különösen a Szahel-övezetben, de Irakban és Szíriában is – tehermegosztásnak tekintik – valamiféle „természetbeni", közvetetten védelmi kiadásként értelmezhető hozzájárulásnak, amely akkor is növeli a NATO és Európa biztonságát, ha nem a NATO vagy az Európai Unió megbízása alapján végzik.[37] A kontinens legaktuálisabb védelmi kihívása vonatkozásában mind az egyes előzmények, tekintettel arra, hogy a franciák a nemzetközi szerepvállalásaik alkalmával már szembesültek az orosz katonai aktivitással (pl. Líbia, Szíria), mind pedig Franciaország európai súlya miatt is vált az orosz–ukrán konfliktus nyugat-európai hangjává. Tekintettel az ország geopolitikai helyzetére és stratégiai ambíciójára, már-már evidenciaként értelmezhető, hogy azok fenntartásának kiemelt tényezője a széles körű képességfejlesztés. Jelen írás keretei között néhány figyelemre méltó példa megragadása lehet cél.

2.2.1. Hálózatalapú hadviselés

A hálózatalapú hadviselés olyan eljárásrendet és stratégiai gondolkodást jelent, amely az összhaderőnemi hadműveletek során képes a leginkább érvényesülni. Abból az alapvetésből indul ki, hogy az erők hálózatos vezetési eszközökkel történő alkalmazása, értelemszerűen a digitalizációval, az elemzés-értékelés és a döntéshozatal kidolgozott mechanizmusaival képes arra, hogy a katonai egységek műveleti hatékonysága a megváltozott hadviselési és biztonsági környezetben is fennmaradhasson. A hatékonyság fundamentuma az időbeliség és a térbeli helyezkedés, ami a hálózatalapú elvek mentén többdimenziós és egyidejű harctevékenységet vár el, ami a kellő technológiai képességekkel utat teremt a hatásalapú műveleteknek. A dimenziók bevonása abban az esetben teljes körű, ha abban a konvencionális szárazföldi-légi-haditengerészeti triász mellett érdemi teret kap az információs és a kibertér, valamint egyre inkább megszilárdul a horizonton az űrhadviselés is.[38]

Fontos ugyanakkor leszögezni (a képességfejlesztés ezen aspektusára helyezkedve), hogy e szemlélet a korszerű technológiát alapfeltételként kezeli, de egyúttal rámutat arra, hogy azok a hálózatalapú alkalmazás nélkül erős korlátok között rekednek, adott esetben be nem váltott várakozások maradnak csak utánuk. A hálózat olyan működési mód, ami egyszerre teszi szükségessé az ellenséges és a saját képességek átfogó vizsgálatát, a harci potenciál felmérését, a stratégiai pontok priorizá-

[37] Ennek kapcsán lásd: Florence Parly: The US-French Relationship in a Changing World. *Atlantic Council,* 2019 (https://www.atlanticcouncil.org/event/the-us-french-defense-relationship-in-a-changing-world-2/).

[38] Ennek kapcsán lásd Ronkovics József: A 21. század hadviselésének néhány főbb jellemzője. *Hadtudomány,* 2009/1–2. szám, 57–62. o.

lását és a hadviselésnek mindezek mentén való megtervezését. Így a hálózatosság mindkét fél szempontjából érvényesül. Az utóbbi célja a saját erők kohéziójának növelése, egyúttal az ellenséges képességek entrópiájának olyan szintre juttatása, aminek eredményeként az élő erő a kulcsfontosságú technikai képességei és információs rendszerei működésképtelenné válnak, harcképessége drasztikusan csökken, így nem képes érdemben folytatni a harctevékenységet. Mindez (beleértve a prevenciós felderítő és tűzképességet) olyan fejlesztések katalizátora, amelyek az összhaderőnemi helyzetelemzés, a harctéri helyzetértékelés és a digitalizált katonai erők vonatkozásában jelennek meg, és formálják a hagyományos hadszínteret, ahol az ellenség szándékától eltérítésének objektívája végleg megelőzheti a fizikai megsemmisítését.[39] A hálózatalapú hadviselés alapvetően az Egyesült Államokban kialakított, de több országban teret nyerő direktíva.

A legfontosabb, hálózatalapú francia fejlesztés a „SCORPION" modernizációs program. A SCORPION a francia hadseregnek a hálózatba kapcsolt hadviselésbe történő, az 1990-es években megkezdett beruházásainak új fordulópontját jelenti, egy olyan jármű-modernizációs programmal kombinálva, amelynek célja az 1970-es és 1980-as évekből származó, régi könnyű járművekből álló flotta lecserélése. A „SCORPION" középpontjában az információs és hálózati technológia áll, amelynek célja, hogy a különböző szinteken lévő összes elemet hálózatba kapcsolja, jelentősen fokozza az információmegosztást, és megkönnyítse a logisztikát a bevetett járművek állapotára és szükségleteire vonatkozó adatok automatikus generálásával. A SCORPION sikerének kulcsa a Thales által gyártott új „CONTACT" rádiós és két információs rendszer – a SCORPION Információs és Harcászati Rendszer, valamint a Système d'Information des Armées (Katonai Információs Rendszer). A SCORPION Információs és Harcászati Rendszer ezredek és kisebb hadosztály nagyságú erők számára készült; a Système d'Information des Armées a hadtestek és hadosztályok szintjén funkcionáló rendszer. Ezekre a rendszerekre számos haditechnikai termék csatlakozik, például a Griffon páncélozott személyszállító és a Jaguar könnyű harckocsi, hálózati és kommunikációs technológiával tervezve, vetronikával (a járműveket figyelő és a járművekre vonatkozó adatokat közlő technológia, amely megkönnyíti a logisztikát és a fenntartást) funkcionálva. A „CONTACT" rendszerhez tartozik az Antares nevű Thales-rendszereleme, ami a járművek tetején helyezkedik el, 360 fokos képet nyújtva a jármű körül, egyúttal arra képesen, hogy érzékelje a rá irányuló távolságmérő és célzólézereket. Az Antares képes lokalizálni a lézer forrását, és azonosítani például, hogy az milyen típusú harcegységtől (gyalogságtól, harckocsitól vagy repülőgéptől) származik. Az azonosítás mellett szintén alkalmas arra, hogy döntési opciókat generáljon a kezelőszemélyzetnek. A hálózatalapú működést kiszolgálván az eszköz egyúttal a „CONTACT"-on keresztül automatikusan

[39] Ennek kapcsán lásd Kun István – Fáy Gyula – Bukovics István: Logikai hadviselés – Kritikus pontok harca. *Hadmérnök.* 2011/4. szám, 189–203. o.

osztja meg az adatokat a hálózattal, így abban mások azonosíthatják, hogy a kötelékben ki van a legoptimálisabb helyzetben ahhoz, hogy az adott harccselekményt végrehajtsa.[40]

2.2.2. Űrképességek fejlesztése

A francia védelmi fejlesztési program 2019-ben 3,6 milliárd eurót fordított az űrbeli képességekre és azok korszerűsítésére; 2025-ig pedig további 700 millió eurót fordítanak erre a területre. Franciaország érdeklődése e terület iránt nem új keletű, mivel az űrbeli képességekbe történő beruházások értéke 2008 és 2014 között is megduplázódott.[41] A 2019-es védelmi űrstratégia a világűrt a stratégiai és katonai szembenállások színterének nevezi.[42] A téma egyik oldalról a szabályozási hiányosságok és a nemzetközi egyezményeknek való megfeleltethetőség miatti aggályok célpontja, másfelől sürgető fejlesztési terület,[43] tekintettel arra, hogy a francia védelmi minisztérium 2018-ban hozta nyilvánosságra, hogy egy orosz műholdat elfogtak, amint a katonai kommunikációra használt francia–olasz Athena-Fidus műholdat kémlelte. Az ekkor tett nyilatkozat arra is kitért, hogy nem csupán a műholdas kommunikáció tartalmának jogtalan megismerése, de alapvetően az ország műholdas képességeinek zavartalan jövőbeni működése is kiemelt veszélybe kerülhet az államok zavaró technológiái okán. A képességfejlesztés indoka emellett az egyre nagyobb mértékű űrszemét kezelése annak érdekében, hogy csökkenthető legyen a katonai és polgári felhasználás szempontjából kritikus műholdak megrongálódásának kockázata.[44]

Franciaország a modernizáció keretében indította útjára az első Composante Spatiale Optique (Optikai Űrkomponens vagy CSO) katonai felderítő műholdat, amelyből három további műhold indult el a korábban használt Helios műholdrendszer

[40] D. Anand – Ch. Raja – E. G. Rajan: Network Centric Warfare – Concepts and Challenges. *CiiT International Journal of Networking and Communication Engineering*, 2011/3. szám, 898–902. o.; Défense: l'armée de Terre va enfin changer ses vieux 'chameaux. *La Tribune*, 2019 (https://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/20141206trib74266ca36/defense-l-armee-de-terre-va-enfin-changer-ses-vieux-chameaux.html); Nicolas Chaligne: Le système d'information du combat SCORPION. *Fantassins.* 2016/36. szám, 48–52. o. (http://www.emd.terre.defense.gouv.fr/img/emd/fantassin/2016_n36_fantassins.pdf).

[41] Murielle Delaporte: From Paris to Orbit: France's New Space Strategy. *Breaking Defense.* 2019. Ministère des Armées, Actualités, Florence Parly Dévoile la Stratégie Spatiale Française de Défense.

[42] Stratégie Spatiale de Défense (https://www.vie-publique.fr/sites/default/files/rapport/pdf/194000642.pdf); Pierre Alonso: L'Armée Française Se Prépare à La Guerre des Étoiles. *Libération.* 2019 (https://www.liberation.fr/france/2019/07/25/l-armee-francaise-se-prepare-a-la-guerre-des-etoiles_1742041/).

[43] Malik Miktar: La France entre dans l'ère de la militarisation de l'espace. *TV5 Monde.* 2019 (https://information.tv5monde.com/info/la-france-entre-dans-l-ere-de-la-militarisation-de-l-espace-313391).

[44] John Irish: France Accuses Russia of Spying on Military from Space. *Reuters*, 2018 (https://www.reuters.com/article/us-france-russia-security-idUSKCN1LN1XT).

leváltására. A CSO-rendszert Franciaország Németországgal, Svédországgal és Belgiummal együttműködve fejlesztette ki, és adatokat szolgáltat a Multinational Space-Based Imaging System (Többnemzeti Űrbázisú Képalkotó Rendszer) számára, amely program lehetővé teszi Franciaország, Belgium, Németország, Görögország, Olaszország és Spanyolország számára az űrből származó felderítési információk megosztását.[45] Franciaország új űrstratégiája folyamatos együttműködést szorgalmaz az Egyesült Államokkal, Európát pedig olyan szereplőként említi, amelynek saját kapacitásokkal kell rendelkeznie, így lehetővé téve, hogy hiteles partnere legyen az Egyesült Államoknak. Ugyanakkor a stratégia azt is világosan kimondja, hogy a katonai térbeli képességek tekintetében a nemzetközi képesség-összevonás korlátozott, mivel a nemzetek megtartják a képességeik feletti szuverén ellenőrzést.[46]

2.2.3. Kibervédelmi és -biztonsági rendszerfejlesztés

A francia katonai kibertevékenység a védelmi fejlesztések egyik központi eleme, akár a hálózatalapú hadviselés ismertetett eszközrendszerére, akár a területre fordított, ismert kiadásokra[47], akár csak a kibertér globális kihívásaira nézünk.[48] Fordulópontként értékelhető a Katonai Kiberstratégia kiadása, amely az első olyan specifikus katonai stratégiai dokumentum, amelynek egyes („A katonai támadó kiberdoktrína nyilvános elemei" és „A védelmi miniszter védelmi politikájának nyilvános elemei") részeit nyilvánossá tették. A nyilvánosságra hozott dokumentumok összhangban vannak a francia Kibervédelmi Stratégia és a Fehér Könyv elgondolásaival, a globális hatalmi szerepvállalás, a defenzív és az offenzív kiberműveleti képességek egyaránt megjelenítésre kerülnek.[49]

[45] Aurent Lagneau: Accord franco-allemand sur les satellites d'observation et la prochaine génération de drones MALE. *Opex360.com*, 2015 (http://www.opex360.com/2015/04/01/accord-franco-allemand-sur-les-satellites-dobservation-la-prochaine-generation-de-drones-male/).

[46] *Stratégie Spatiale de Défense*, Paris, 2019. 38. o.

[47] Vincent Lamigeon: Budget des Armées 2019: Qui Sont les Gagnants? *Challenges*, 2018.

[48] Ennek kapcsán lásd Spitzer Jenő: A francia kibervédelmi és -biztonsági rendszer egyes stratégiai aspektusai. *Military and Intelligence CyberSecurity Research Paper* 2021/3. szám, 1–16. o.; Dave Clemente: Cyber Security and Global Interdependence: What Is Critical? London, The Royal Institute of International Affairs, 2013; Kelemen Roland – Simon László: A kibertérben megjelenő fenyegetések és kihívások kezelésének egyes nemzetközi jogi problémái. In Farkas Ádám – Végh Károly (szerk.): *Új típusú hadviselés a 21. század második évtizedében és azon túl – intézményi és jogi kihívások.* Budapest, Zrínyi Kiadó, 2020, 150–170. o.; Kelemen Roland: A kibertérből érkező fenyegetések jelentősége a hibrid konfliktusokban és azok várható fejlődése. *Honvédségi Szemle,* 2020/4. szám, 65–81. o.; Kelemen, Roland – Farkas, Ádám: To the Margin of the Theory of a New Type of Warfare: Examining Certain Aspects of Cyber Warfare. In Szabó, Marcel – Gyeney, Laura – Láncos, Petra Lea (szerk.): *Hungarian Yearbook of International law and European Law (2019).* Den Haag, Eleven International Publishing, 2020, 203–226. o.

[49] Fehér Könyv 53. o.

A Kibervédelmi Stratégia pillérei az elrettentés, a védekezés, a megelőzés és a fellépés, a megismerés és az előrejelzés.[50] Mindez egyfelől determinálja a szervezeti kereteket és a funkciókat, másfelől a fellépés, a megismerés és az előrejelzés követelményéből arra következtethetünk, hogy a francia kibervédelem magában foglalja a nemzetbiztonsági közreműködését. A francia kibervédelem a következő szervezeti strukturában realizálódik:

- az Információs Rendszerek Biztonságáért Felelős Nemzeti Ügynökség (ANSSI[51]), amely az állam kibervédelméért és a defenzív kibertevékenység legfelső szintű koordinációjáért és technikai felügyeletéért – a miniszterelnök felügyelete alá utalva – felelős;
- a védelmi miniszter irányítása alá tartozó Kibervédelmi Parancsnokság (COMCYBER[52]), mint operatív elem;
- a védelmi miniszter irányítása alá tartozó nemzetbiztonsági szolgálatok (DGSE[53], DRSD[54], DRM[55]) és
- a belügyminiszter szakosított nemzetbiztonsági szolgálata (DGSI[56]).[57]

2.3. Nagy-Britannia (PwrIndx: 0.1382, 8. helyezés)

Az Egyesült Királyság Franciaországot szorosan követi katonai képességeiben, Európa meghatározó katonai szereplőjeként tartandó számon. Katonai képessége és geopolitikai súlya nagyban determinált arra nézve is, hogy számottevő atomfegyverrel bír.[58]

2030-ig tartó stratégiai elképzelésében a brit kormány evidenciaként kezeli a globális hatalom jellegének és eloszlásának megváltozását és a kompetitív dinamikát hozó multipoláris világrend kiszélesedését. Ezek vonatkozásában négy fő aspektust határoz meg:

[50] Lásd Alix Desforges: *Approche géopolitique du cyberespace, enjeux pour la défense et la sécurité nationale, l'exemple de la France.* Thèse, Université Paris, 2018.

[51] *Agence nationale de la sécurité des systèmes d'information.* A nemzetbiztonsági szolgálatok nemzetközi áttekintése kapcsán lásd Béres János (szerk.): *Külföldi nemzetbiztonsági szolgálatok.* Budapest, Zrínyi Kiadó, 2018, 103–107. o.

[52] *Commandement de la cyberdéfense.*

[53] *Direction générale de la sécurité extérieure* (Külső Biztonsági Főigazgatóság).

[54] *Direction du renseignement et de la sécurité de la défense* (Katonai Hírszerzési és Védelembiztonsági Igazgatóság).

[55] *Direction du renseignement militaire* (Katonai Felderítő Igazgatóság).

[56] *Direction générale de la sécurité intérieure* (Belbiztonsági Főigazgatóság).

[57] Spitezer: i. m. (2021), 3. o.

[58] Ennek kapcsán lásd: Status of World Nuclear Forces – Who owns the world's nukes? Federation of American Scientist (https://fas.org/issues/nuclear-weapons/status-world-nuclear-forces/).

- a geopolitikai és geoökonomiai változásokat (például Kína növekvő nemzetközi befolyása, az Indo-csendes-óceáni térség növekvő jelentősége a globális jólét és biztonság szempontjából, valamint az új piacok megjelenése és a globális középosztály növekedése);
- az államok közötti és a nem állami szereplőkkel folytatott verseny fokozódása (a nemzetközi szabályok és normák feletti növekvő verseny; egymással versengő geopolitikai és gazdasági befolyási és értékblokkok kialakulása; a demokratikus rendszerek gyenge pontjainak tudatos célbavétele az autoriter államok és rosszindulatú szereplők által; valamint a háború és béke közötti határvonal szándékos tesztelése);
- felgyorsuló technológiai fejlődés és digitalizáció (egyidejűleg a tudomány és a versenypiac hatásgyakorlásával);
- transznacionális kihívások (éghajlatváltozás, globális egészségügyi kihívások, terrorizmus).[59]

E palettát figyelembe véve az alábbi fejlesztési területek emelhetők ki:

Kutatás-fejlesztés

A brit kormány arra nézve vállalt kötelezettséget, hogy 2027-ig a GDP legalább 2,4%-át K+F-re fordítja. Ez a fajta védelmi befektetés olyan technológiai és tudományos lépéstartásnak tekinthető, aminek eredményeként az Egyesült Királyság a modern platformok és fegyverrendszerek vonatkozásában célként jelöli meg a stratégiai előny elérését, legyen szó a kibertérről, a felfegyverzett drónok alkalmazásáról, az űrhadviselésről, vagy akár nagy hatótávolságú precíziós fegyverekről.[60]

Az Egyesült Királyságban számos technológiai klaszter működik, de kiemelt figyelmet érdemel a Védelmi Innovációs Központok hálózata[61], amely a Védelmi Minisztérium részeként működik. Feladata, hogy védelem és a biztonság témakörében kapcsolja össze a kormányzat, a magánszektor és az akadémiai közeg kutatóit, létrehozva egy olyan közeget, ahol az ágazati modernizáció eredményessége épp a többoldalú megközelítés konszenzusából teremtődik meg.

[59] The Integrated Review of Security, Defence, Development and Foreign Policy (A biztonság, a védelem, a fejlesztés és a külpolitika átfogó felülvizsgálatáról szóló kiadványa) 23–33. o. (https://tinyurl.com/5cduh34p).

[60] Ministry of Defence: The Defence and Security Public Contracts Regulations (DSPCR) Chapter 10: research and deelopment. 2022. november 10. (https://www.gov.uk/government/publications/the-european-union-defence-and-security-public-contracts-regulations-dspcr-2011/dspcr-chapter-10-research-and-development#what-is-the-legal-framework); Lásd még: Research and development expenditure by the UK government: 2020. (https://www.ons.gov.uk/economy/governmentpublicsectorandtaxes/researchanddevelopmentexpenditure/bulletins/ukgovernmentexpenditureonscienceengineeringandtechnology/2020).

[61] The Defence and Security Accelerator. (https://www.gov.uk/government/organisations/defence-and-security-accelerator).

A hosszú távú stratégia részeként a K+F mellett tesztelési és értékelési (T&E) képességek kialakítása is tervezett annak érdekében, hogy az újszerű fegyverek, a mesterséges intelligencia, a digitális rendszerek és az űrbe telepített rendszerek gyakorlati szempontú vizsgálata is teret kapjon. Ezek a területek a T&E Futures program keretében kerülnek kialakításra, amelybe a következő négy évben több mint 60 millió fontot fektet a brit kormány. Mindettől a következő generációs technológiáknak a mihamarabbi felhasználói szintre jutását remélik.[62]

Az Egyesült Királyság Tudományos és technológiai stratégiája meghatározza azokat legsürgetőbb területeteket, ahol a képességfejlesztés döntő előnyt biztosíthat a jövőben:

- az átfogó, teljes spektrumú hírszerzés és felderítés,
- összhaderőnemi vezetés és irányítás, kommunikációs és technológiai szempontból,
- az adatok hatékony megosztása,
- aszimmetrikus hadviselés.[63]

A fentiek tekintetében a célok és eszközök összefogására egy Stratégiai Parancsnokság[64] hivatott, amely egy digitális átalakítási programot vezet, megerősítve egy olyan digitális gerinchálózattal, amely az információk kiaknázására optimalizált és a több területre kiterjedő integrációt lehetővé tevő digitális infrastruktúraként megalapozza fegyveres erőink modernizációját, valamint támogatja a védelmi képességek szélesebb körű átalakítását. Ez magában foglalja a műszaki és logisztikai támogató rendszerek korszerűsítését, az eszközök és a személyi állomány rendelkezésre állásának valós idejű ismeretét. A gerinchálózattal szembeni elvárások többek között a NATO-val és a legfontosabb egyéb szövetségesekkel való közvetlen és folyamatos kapcsolattartás, a felhőalapú kommunikáció lehetősége, valamint a kormányzati rendszer egészébe való integráltság. Ezeket a követelményeket a Digitális Védelmi Stratégia fekteti le.[65]

[62] Research and Development funding policy (https://researchbriefings.files.parliament.uk/documents/CBP-7237/CBP-7237.pdf).

[63] Science and Technology Strategy 2020. Ministry of Defence. 21–35. o. (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/927708/20201019-MOD_ST_Strategy_2020_v1-23.pdf).

[64] Strategic Command (https://www.gov.uk/government/organisations/strategic-command).

[65] Digital Defence Strategy. 14–29. o. (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/990114/20210421_-_MOD_Digital_Strategy_-_Update_-_Final.pdf).

2.3.1. Kibertér

Az Egyesült Királyság e szegmensben leginkább említésre méltó fejlesztési lépése a Nemzeti Kiber Erők (National Cyber Force, NCF) létrehozása. A szervezet létrehozása a Védelmi Minisztérium keretében került végrehajtásra, együttműködésben a Kormányzati Kommunikációs Központtal (Government Communications Headquarters, GCHQ[66]) és az MI6-szel[67], továbbá partnerségben áll a bűnüldöző szervekkel is.

Az NCF képességeket biztosít, defenzív és offenzív fellépést jelent a kibertérből érkező támadások, a diszruptív technológiák és a dezinformáció vonatkozásában, ezeket pedig jelentős titkosszolgálati háttértámogatással képes folytatni. Ez utóbbiaknak integrált infomációs bázist és operatív technikai szakértelmet képes biztosítani.

A kibertér a részét képezi a nagyobb halmazként kezelendő elektromágneses környezetnek, védelmi fejlesztéseiben az Egyesült Királyság ennek az átfogó értelmezésére törekszik.[68]

2.3.2. Űrkutatás

A brit kormány deklarált célja, hogy 2030-ra az Egyesült Királyság képes legyen az űrben és az űrön keresztül információt szerezni és megvédeni érdekeit, a nemzeti képességek és a szövetségeseinkkel való partnerségek ötvözésével.

Ennek támogatására került megvalósításra a Skynet 6 program, amelyhez kötődően a következő 10 évben mintegy 5 milliárd fontot fordítanak műholdas kommunikációs képességeink feltőkésítésére és fejlesztésére, és a következő évtizedben további 1,4 milliárd fontot fordítanak az űrkutatásra. Kiemelt sarokpontok a következők:

- új űrparancsnokság létrehozása,
- a kereskedelmi űrtevékenység koordinációjának segítése és az új űralapú képességek fejlesztése,
- az űrterület tudatosságának fokozása, beleértve egy nemzeti űrkutatási központ létrehozását,
- űrműveleti központ létrehozása, az ellenséges hírszerző és katonai tevékenységekkel kapcsolatban,
- hírszerző, megfigyelő és felderítő műholdkonstelláció kifejlesztése, ehhez kapcsolódóan egy támogató digitális gerinchálózatot létrehozása, valamint
- űrakadémia létrehozása a védelmi űrspecialisták képzésére.[69]

[66] A GCHQ a brit titkosszolgálatok egyike, amelyik képi felderítéssel és információvédelemmel kapcsolatos feladat- és hatáskörökkel rendelkezik.

[67] *Secret Intelligence Service* (SIS), az Egyesült Királyság katonai hírszerző titkosszolgálata.

[68] Ennek kapcsán lásd: Joint Doctrine Note 1/18 Cyber and Electromagnetic Activities. Ministry of Defence (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf).

[69] Ennek kapcsán lásd George Allison: UK aims to become 'meaningful player in space. *UK Defence Journal.* 2021 (https://ukdefencejournal.org.uk/uk-aims-to-become-meaningful-player-in-space/).

2.4. Németország (PwrIndx: 0.2322, 16. helyezés)

Németország esetében a képességfejlesztési törekvések vonatkozásában három trendet emelnénk ki. Az első a fegyveres erők fejlesztési koncepciójának tervszerű felépítése és a végén az ukrán–orosz konfliktusnak is köszönhető, európai szinten is kimagasló mértékű védelmibüdzsé-emelés. A következő, szinte természetesen a kibervédelem stratégiai megközelítésének és szervezeti változásainak bemutatása. Végül pedig, sajátos jogi és etikai értékelése miatt a részben már meglévő drónok felfegyverzéséről szóló vitát mutatjuk be röviden.

A német fegyveres erők képességfejlesztése egy alapos stratégiai-tervezési folyamatot követően egy aránylag hosszú időtávra tervezett. 2016-ban fogadták el az ún, Fehér Könyvet, a biztonságpolitikáról és a Bundeswehr jövőjéről.[70] Ebben elsősorban a „hová" kérdésre igyekeztek válaszokat megfogalmazni a stratégiai prioritások, a hadsereg céljainak és feladatainak meghatározásával. Ez a programadó alapdokumentum több lényeges újítást hozott a német biztonság- és védelempolitikába, meghaladva többek közt olyan korábbi tabukat, mint a nemzeti hadseregben való szolgálat megnyitása más uniós államok polgárai előtt.[71]

A Bundeswehr koncepcióját[72] a Fehér Könyv irányelvei alapján 2018 nyarán fogadták el, és a „hogyan" kérdésre válaszokat adva tovább konkretizálta a végrehajtandó feladatokat és célkitűzéseket, a feladatspektrum differenciálásával és a képességprofil kidolgozásához szükséges előfeltételek megfogalmazásával.

A Bundeswehr – az előző kettőtől eltérően már zártan kezelt – képességprofilját ezután már viszonylag gyorsan, 2018 szeptemberében mutatta be a hadsereg főszemlélője, és a „mivel" kérdést fókuszba hozva konkrét terveket, előírásokat és válaszokat adott a fegyveres erők felszerelésére, és éves bontásban jelenítette meg az elvárt, programszerű előrehaladást. Tudható, hogy a fő mérföldkövei 2023, 2027 és 2031. Az első időpontra németek által, a NATO kereteiben vezető keretnemzetként kiállítandó VJTF (Very High Readiness Joint Task Force) magas készültségi szintű és gyorsreagálású harccsoport kiállítása a fő feladat. 2031-re a kitűzött ambíciószint korszerűen felszerelve három szárazföldi hadosztály, 4 légierő-harccsoport, egy 25 felszíni egységből és 8 tengeralattjáróból álló haditengerészet, potens kibervédelmi erők, különleges műveleti és világűrképesség és a szükséges támogató csapatok megléte (vegyvédelem, logisztika, műszaki stb.).

A fenti fejlesztési folyamatot a GDP-arányos védelmi költségvetés folyamatos növelésével (2024-re kívánták elérni a 1,5%-ot) tervezték végrehajtani. Az ukrán–

[70] *Weissbuch 2016 zur Sicherheitspolitik und zur Zukunft der Bundeswehr*, 36–38. o. (https://www.bundesregierung.de/resource/blob/975292/736102/64781348c12e4a80948ab1bdf25cf057/weissbuch-zur-sicherheitspolitik-2016-download-data.pdf).

[71] *Weissbuch 2016* 120. o.

[72] *Konzeption der Bundeswehr*, 29–30, 43–44, 52. o. (https://www.bmvg.de/de/aktuelles/konzeption-der-bundeswehr-26384).

orosz háború viszont drasztikus változást hozott, olyannyira, hogy 2022 júniusára már a Bundestag mindkettő háza elfogadott egy 100 Mrd eurós fejlesztési programot,[73] amely egyébként az alaptörvényben rögzített eladósodottsági ráta emelése miatt kétharmados döntést igényelt, és Olaf Scholz kancellár már a 2%-os költési szint eléréséről és fenntartásáról beszélt. A keretből 2 Mrd a katonák egyéni felszerelésére, ruházatára, 20,7 a vezetési technológiákra, digitalizált és rejtjelezett kommunikációra, 40,8 Mrd a légierő képességfejlesztésére (F-35-ös 5. generációs vadászbombázók, új CH-47-es helikopterek), 16,6 Mrd a szárazföldi erőkre és 19,3 Mrd a tengerészetre lett betervezve.[74]

A már tárgyalt Bundeswehr-koncepció szerint az összkormányzati biztonság és integritás a kiber- és információs térben és az ehhez szükséges katonai informatikai rendszerek reziliens alkalmazása, üzemeltetése és védelme alapfeladat. A Bundeswehr szerepe és feladatai az aktuális német kibervédelmi stratégiából, illetve egyes aspektusok a hadsereg alkotmányban meghatározott országvédelmi feladataiból eredeztethetőek. Idesorolható a kritikus infrastruktúrák védelme, vagy támadások esetén a műveleti képesség megőrzése a kibertérben. A kiberbiztonság védelempolitikai vonatkozásai és ezek nemzetközi kontextusú értelmezése kapcsán a Bundeswehr a NATO-keretekhez orientálódik. A hadseregnek a jövőben készen kell állnia komplex kibertámadások elhárítására, defenzív és offenzív képességekre is szüksége van, melyeket folyamatosan készenlétben kell tartania, és fejlesztenie kell. Az innovációs sebesség és a fenyegetések globális minősége is megköveteli a nemzeti és nemzetközi partnerekkel való együttműködést a gazdasági, tudományos és innovációs szférából.

Az első német kiberbiztonsági stratégiát 2010-ben fogadták el, a jelenleg hatályos szöveg 2021-ban készült el. Legfontosabb új irányai a stratégia egyes intézkedések hatékonyságának növelése és mérhetővé tétele lett. Hangsúlyos szerepet kap a „security by design"-elv erősítése (az IT termékekbe előre betervezett biztonság), és még inkább elmélyíti a kapcsolatokat a tudományos és a gazdasági szféra irányában. A vállalkozások fokozott védelme szintén erősítendő, ahogy az is, hogy az üzemeltetők mellett a gyártók és beszállítók szerepét is figyelembe kell venni biztonsági kérdésekben. A kritikus infrastruktúrák erősebb bevonása mellett emelni szükséges az összkormányzati kiberbiztonsági architektúra színvonalát, és a minél hatékonyabb fellépése érdekében megfelelően kell pozicionálni a Szövetségi Információtechnikai Biztonsági Hivatalt (BSI),[75] ami azóta törvénymódosítással meg is történt.

[73] Ja vom Bundesrat: Milliarden für Bundeswehr. *ZDF Heute*. 2022 (https://www.zdf.de/nachrichten/politik/bundeswehr-sondervermoegen--grundgesetz-bundesrat-100.html).

[74] Bundeswehr-Sondervermögen: Wohin gehen die 100 Milliarden? *ZDF Heute*, 2022 (https://www.zdf.de/nachrichten/politik/bundeswehr-sondervermoegen-waffen-liste-100.html).

[75] Dennis-Kenji Kipker: *Cybersecurity Regulierung 2021: Update* (https://www.researchgate.net/publication/348365761_Cybersecurity-Regulierung_2021_ Update).

Miután 2017 áprilisában a kiber- és információs teret a hadsereg legújabb szervezési területeként azonosították (a hagyományosnak tekinthető szárazföldi, légvédelmi és tengeri területek mellett), 2021-es határidővel kialakították a Bundeswehr új feladatának ellátásához szükséges szervezeti hátteret is, tervezetten 14 500 fős állománnyal. A doménfelelősség keretében el kell látni a hadsereg belföldi és missziós IT-rendszereinek védelmét, biztosítani kell a szükséges felderítést és üzembiztosságot, a szükséges geoinformációs adatokat, és a szakterületi kapcsolattartást más kibertémában felelős szervekkel. Le kell szögezni azonban, hogy a nemzeti szintű védelmi képességfejlesztés és megóvás szempontjából kulcsfontosságú a Bundeswehr viszonylatában a BAMAD támogatása és feladatellátása a haderő nemzetbiztonsági jellegű védelmének és stabilitásának erősítése érdekében. A hadsereg informatikai képességeit egy vezető és két alárendelt parancsnoksághoz osztották be:

- Kiber- és Információstér Parancsnokság (Kommando Cyber- und Informationsraum, KdoCIR);[76]
- Információtechnikai Parancsnokság (Kommando Informationstechnik, KdoITBw);[77]
- Stratégiai Felderítési Parancsnokság (Kommando Strategische Aufklärung, KdoStratAufkl).[78]

A Bundeswehr parancsnokságai és a BAMAD (katonai elhárítás, Bundesamt für den Militärischen Abschirmdienst[79]) a (katonai) kibervédelemre koncentrál, a haderő szerepköre pedig a NATO-fejlesztésekkel is szoros szinkront mutat, és a kiberen túl az információs műveletekkel is összekapcsolódik. Látni kell azonban a tagállami és szövetségi szintű kormányzati irányítás, illetve a koordináció rendszeréből, továbbá a parancsnokságok és a BAMAD alapfeladataiból, hogy ez a képességfejlesztés nem önálló működést hoz létre, hanem egy komplex összkormányzati, ezáltal politikai-igazságügyi-nemzetbiztonsági-katonai mátrixban megjelenő fontos részrendszerként írható le.

A polgári-katonai párhuzamosság és a kormányzati szerveken is túlnyúló hálózatosság a német rendszerben is alapvetés a kiberbiztonság terén, a szakterületek és a szereplők közötti szoros kooperációval. Az egyes szervezetek és szférák (állami, gazdasági és civil) között több koordinációs és kooperációs megoldás is biztosítja a rendelkezésre álló információk megosztását, a legjobb gyakorlatok terjedését. Kü-

[76] A szervezetről lásd: https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/kommando-cyber-und-informationsraum.

[77] A szervezetről lásd: https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/kommando-informations technik-der-bundeswehr.

[78] A szervezetről lásd: https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/kommando-strategische-aufklaerung.

[79] A szervezetről lásd: https://www.bundeswehr.de/de/organisation/weitere-bmvg-dienststellen/mad-bundesamt-fuer-den-militaerischen-abschirmdienst.

lönösen nagy hangsúlyt kap a lényegi tudás összegyűjtése, rendszerezése, és azok eljuttatása az érintettekhez a legkülönfélébb csatornákon keresztül.

A német kibervédelmi felfogás kifejezetten defenzív alapállású, az idegen rendszerekbe történő behatolásra – hivatalosan – csupán korlátozott körben, az attribúció megállapítása vagy bűnüldözési, forenzikus szempontok miatt kerülhet sor. 2017 környékén még aktív szakmai vita folyt arról, hogy szabad-e egyáltalán offenzív kiberképességeket kiépíteni. Egyes megközelítések szerint ezek a fegyveres erők védelemközpontú alapállásával ellentétesek, másrészt alkalmazásuk a konfliktusok további eszkalációjához vezethetnek.[80] Ellenvéleményként az merült fel már akkor is, hogy a fenyegetettség növekedése miatt az ortodox defenzív álláspont nem tartható, a kritikus infrastruktúrák védelme megköveteli hogy szükség esetén ütőképes legyen a védelmet ellátó szervezet, és amennyiben szükséges, akár a megfelelő jogi háttér megteremtésével is lehetővé kell tenni a hatékony fellépést az ország érdekében.[81] Azóta a 2021-es kiberbiztonsági stratégia már nyíltan tételez offenzív képességeket, és Ukrajna megtámadása miatt sem várható, hogy újra teret kapna egy túl óvatos megközelítés.

Alapjogi természete miatt kiemelendő a 2020-as évben egy másik kiberbiztonsági téma, amely inkább a német kormányzat nemzetbiztonsági tevékenységével volt összefüggésben. A világ legforgalmasabb internetcsomópontja a frankfurti DE-CIX[82], amely már napi 91 terrabit adatot is továbbított. Nem meglepő módon a német hírszerzés (BND) is figyelemmel kíséri ezt a csomópontot – és sokáig lényegi korlátozások nélkül tette mindezt. 2020. május 19-ig döntésében a német Szövetségi Alkotmánybíróság kimondta, hogy a külföldi állampolgárok külföldi telekommunikációs forgalmát ugyanúgy megilleti a telekommunikációs titok védelme, ezért az addig folytatott kiterjedt megfigyelési programját a BND-nek le kellett állítania, és az döntésnek megfelelő fokozottabb felügyelet mellett és korlátok között 2021 végéig kell a törvényhozásnak az alkotmánnyal konform új szabályozást megalkotnia.[83]

Nemzeti jogi és alkalmazható haditechnika szempontjából egy másik fontos, etikai vonzatokkal bíró vita volt a hadsereg által vásárolt drónok (UAV, Unmanned Aerial Vehicle) felfegyverzése. A kérdésnek tulajdonított jelentőséget jól jelzi, hogy a

[80] Példaként lásd Stefan Heumann: Cyberkrieg und die Bundeswehr – Warum Cyber-Gegenangriffe gefährlich sind. *Tagespiegel Causa*. 2017 (https://causa.tagesspiegel.de/politik/darf-die-bundeswehr-cyber-attacken-zur-verteidigung-nutzen/warum-cyber-gegenangriffe-gefaehrlich-sind.html.)

[81] Példaként lásd: Martin Schallbuch: Cyber-Angriffe der Bundeswehr – Eine Cyber-Armee braucht auch einen Auftrag. *Tagesspiegel Causa*. 2017 (https://causa.tagesspiegel.de/politik/darf-die-bundeswehr-cyber-attacken-zur-verteidigung-nutzen/eine-cyber-armee-braucht-auch-einen-auftrag.html.)

[82] Sven Lilienström: Jeder kann einen Cyber-Angriff für weniger als 18 Euro beauftragen. *The European*. 2020 (https://www.theeuropean.de/sven-lilienstroem/cybersicherheit-in-deutschland/).

[83] Ausland-Ausland-Fernmeldeaufklärung nach dem BND-Gesetz verstößt in derzeitiger Form gegen Grundrechte des Grundgesetzes. *Bundesverfassungsgericht*. 2020. (https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2020/bvg20-037.html).

2018-as CDU, CSU és SPD koalíciós szerződés kimondta, hogy a Bundestag csak egy kiterjedt nemzetközi jogi, alkotmányjogi és etikai vizsgálatot követően hozhat majd döntést a kérdésben. A vitaanyagot a kezdeményezőként fellépő Szövetségi Védelmi Minisztérium állította össze, és részletes érvelésében a drónok felfegyverzését javasolta éppen a saját csapatok védelme és a korszerű eszközökön keresztül a járulékos veszteségek csökkentése érdekében. Ezzel együtt az alkalmazáshoz egy részletes előfeltétel-rendszert is megadtak, például a Rules of Engagement (művelet-végrehajtási szabályok) megfelelő kialakítása, a bevetésre vonatkozó parancs kiadásának pontos leszabályozása, a körültekintő alkalmazáshoz elengedhetetlen kiképzés elvégzése.[84] 2022 áprilisában a Bundestag védelmi bizottsága ez alapján már hozzájárult a 140 darab Izraeltől beszerzett Heron típusú drónból 80-hoz fegyverzet beszerzéséhez, azzal, hogy a részleteiben kidolgozott bevetési feltételeket a kormányzatnak össze kell állítania, majd a védelmi és külügyi bizottságnak jóvá kell hagynia azt.[85]

2.5. Svájc (PwrIndx: 0.5015, 32. helyezés)

Svájc világhatalmi szempontból történő megközelítésének első kilométerköve az immár több évszázados függetlensége, ami a szövetségesi rendszerekből való kimaradását jelentette, de nem eredményezte az azoktól való érintettség elmaradását. Részben az ország méretének, részben az elmúlt időkben a nyugati trendekhez igazodó, védelmi fejlesztéseket érintő megtorpanásának és alapvetően a nyugati kultúrkörhöz való tartozásának velejárója a kapcsolat, amire kiváló példa a NATO Békepartnerség államai közé tartozás, valamint az is, hogy a közelmúltban Oroszországgal szemben az ukrajnai tevékenységei miatt kiszabott szankciók érvényre jutásában Svájc is kiállt.[86]

A 2021-es Biztonságpolitikai Jelentés még az ukrajnai orosz invázió előtt készült, így várhatóan a benne foglaltak átértékelésre kerülhetnek, ugyanakkor az anyag

[84] Bericht des Bundesministeriums der Verteidigung an den Deutschen Bundestag zur Debatte über eine mögliche Beschaffung bewaffneter Drohnen für die Bundeswehr (https://www.dbwv.de/fileadmin/user_upload/Mediabilder/DBwV_Info_Portal/Blickpunkt/2020/07_Juli/20200703-BMVg_Bericht_bewaffnete_Drohnen.pdf).

[85] Bundestagsausschuss stimmt Bewaffnung von Drohnen zu. *Welt.* 2022 (http://www.welt.de/politik/ausland/article238020967/Bundeswehr-Bundestagausschuss-stimmt-Bewaffnung-von-Drohnen.hu.html).

[86] Az ország kommunikációjában ilyenkor sokkalta inkább a nemzetközi béke és biztonság, mint az ENSZ alapokmányából fakadó terminus válik hivatkozási alappá és nem egy-egy szövetségesi rendszer (egyébként ugyanebből az alapértékből fakadó) értékrendje. Svájc függetlensége kapcsán lásd Sibilla Bondolfi: How neutral is Switzerland, really? *Swissinfo.* 2022 (https://www.swissinfo.ch/eng/focus-page-foreign-policy_how-neutral-is-switzerland--really-/45810276); Daniel Warner: Goodbye (Swiss) neutrality? *Swissinfo.* 2022. (https://www.swissinfo.ch/eng/goodbye--swiss--neutrality-/47823256).

Oroszország tevékenységéből akkor is prognosztizált komolyabb szembenállást.[87] A svájci katonapolitika kulcskérdéseiként a következők állapíthatók meg:

1. Milyen katonai képességekkel kell rendelkeznie Svájcnak a szuverenitása megóvása érdekében, tekintettel a semlegességére és az a körüli vitákra (NATO és EU felé közeledés[88])?
2. Milyen mértékben és milyen keretek között járuljanak hozzá a svájci fegyveres erők Európa biztonságához?
3. Milyen tanulságok vonhatók le a jelenlegi háborúból a svájci fegyveres erők számára, illetve hogyan alakulnak át a védelmi és biztonsági prioritások a jövőre nézve?[89]

Svájc védelmi költségvetése az előrejelzések szerint a 2022-es 9,44 milliárd dollárról 2027-re 10,35 milliárd dollárra nő, a finanszírozás pedig a beszerzések, a műveletek és egyéb járulékos költségek, köztük a képzés, a nyugdíjak, a hírszerzési tevékenységek és a különféle szolgáltatások között oszlik meg. A beszerzésekre szánt költségvetési előirányzat tovább nőtt, a 2018-as 1,5 milliárd dollárról 2022-re 2,2 milliárd dollárra emelkedett, és a GlobalData előrejelzése szerint 2027-re eléri a 2,6 milliárd dollárt. Az előrejelzési időszakban a svájci védelmi kiadások fő mozgatórugója a légvédelmi erők modernizálásának szükségessége lesz, hogy biztosítsa területének folyamatos védelmét a külső fenyegetésekkel szemben. Az Air2030 program 5. generációs vadászrepülőgépekkel fogja ellátni Svájcot, amelyek képesek lesznek reagálni a svájci légtérben jelentkező fejlett fenyegetésekre. Svájc semleges státusza ellenére a hosszú távú költséghatékonyság, valamint az európai biztonság romlása miatti növekvő aggodalmak indukálják a légvédelmi flotta felszereléséhez szükséges fejlett platformok beszerzését. Ugyanakkor amíg a NATO-tagokra egyre nagyobb nyomásként nehezedik, hogy bruttó hazai termékük 2%-át költsék védelemre, Svájcnak nincs hivatalos kötelezettsége, hogy elérje ezt a küszöböt. A GlobalData szerint a svájci védelmi kiadások 2022-ben a GDP 1,29%-át tették ki, és 2027-re 1,31%-ra fognak emelkedni. Az interoperabilitás, az összekapcsolhatóság és a modularitás kulcsfontosságú a svájci hadsereg legtöbb folyamatban lévő beszerzési programjában: az új platformok és rendszerek, mint például az F-35A vadászgépek, az Eagle V 6×6 felderítő járművek és a Parrot ANAFI drónok mindegyike rendelkezik fejlett

[87] Ennek kapcsán lásd: The security policy of Switzerland 2021. Federal Department of Defence Civil Protection and Sport DDPS (https://www.vbs.admin.ch/en/documents/search.detail.document.html/vbs-internet/en/documents/security-policy/security-reports/2021/sipol-b-2021-e.pdf.html).

[88] Példaként említhető, hogy 2019-ben Svájc tagja lett a NATO Együttműködő Kibervédelmi Kiválósági Központjának (Cooperative Cyber Defence Centre of Excellence), amely az észtországi Tallinnban működik.

[89] Ennek kapcsán lásd Georg Hasler: Why do the Swiss Armed Forces need more money? *Neue Zürcher Zeitung.* 2022 (https://www.nzz.ch/english/why-do-the-swiss-armed-forces-need-more-money-ld.1683332).

adathálózati megoldásokkal, amelyek elősegítik a hálózatalapú hadviselést.[90] Ezzel kapcsolatban az is kiemelendő, hogy a védelmi szektor jelentős és átfogó kommunikációtechnikai fejlesztési programon megy keresztül.[91]

2.6. Figyelemre méltó lépések más országokban

A fenti országok mellett kiegészítésképp még két olyan érdekes irányvonalra szeretnénk felhívni a figyelmet, ami igazán jól illusztrálja azt, hogy egyrészt a 21. század hadviselése mennyire komplex, multi-domain környezet, amely korábban axiomatikusnak vett haderőnemi korlátokat is átlép, másrészt, hogy a high-tech környezet által megkövetelt magas képzettségű állomány iránti igény milyen sajátos – akár a meglévő hadijogi kereteket is feszegető – megoldásokhoz vezethet.

2022 márciusában jelent meg a hír,[92] hogy Szingapúr (PwrIndx: 0.6253, 42. helyezés) a szárazföldi, légi- és haditengerészeti erői mellé negyedikként 2022 utolsó negyedévére prognosztizáltan felállítja a hadseregének Digital and Intelligence Service elnevezésű ágát. Kifejezetten a kibertérből érkező támadásokkal, hibrid fenyegetésekkel és az információs-pszichológiai hadviseléssel lesz a felelősségi területe, de kap felderítési feladatokat is (elsődlegesen a digitális domainben), ami vélhetően azért nem érinti majd a „hagyományos" nemzetbiztonsági szolgálatok portfólióját (Security and Intelligence Division – hírszerzés, Internal Security Department – elhárítás).

Megközelítésük szerint a jövő domináns domainje a kibertér lehet, az onnan jövő fenyegetések a való világban is hatással vannak. A döntés meghozatalakor erősen támaszkodtak az ukrán konfliktusra mint példára. Az átszervezés bázisát a Defence Cyber Organisation a védelmi szféra jelenlegi kibervédelmi szervezete adja, de – képletesen szólva – a jelenlegi „zászlóalj" méretet néhány „dandár" méretre akarják növelni, ezért jön létre a 4. haderőnem – amelynek szervezeti felépítésére egyébként a szintén újdonságnak számító német kiberparancsnokságot hozták példaként. A tervezett beosztásokban nemcsak IT-szakértők, de adat-

[90] Switzerland's defense budget to reach $10.35 billion in 2027 as country acquires more capability from international companies. *GlobalData.* 2022 (https://www.globaldata.com/media/aerospace-defense-security/switzerlands-defense-budget-reach-10-35-billion-2027-country-acquires-capability-international-companies-says-globaldata/).

[91] Armed Forces Telecommunications – Decision made on the model/supplier for the replacement of mobile radio devices, on-vehicle intercom systems and headsets. Federal Department of Defence, Civil Protection and Sports DDPS (https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-76838.html).

[92] Lim Min Zhang: Budget debate: SAF to set up fourth service as digital threats mount, says Ng Eng Hen. *The Straits Times.* 2022 (https://www.straitstimes.com/singapore/politics/budget-debate-saf-to-set-up-fourth-service-as-digital-threats-mount-says-ng-eng-hen).

tudósok, pszichológusok, nyelvészek, antropológusok, földrajztudósok is lesznek, hogy megértsék és elemezzék a komplex fenyegetési környezetet. Ehhez kapcsolódóan egyébként a jövőben a teljes haderő sokkal hálózatosabban végzi majd a kiképzéseit és műveleteit a jövőben.

Észtországot (PwrIndx: 2.6527, 108. helyezés) a 2007-es kiterjedt kibertámadások ébresztették rá, hogy ilyen helyzetekben a békeidei, magas színvonalú képzést, tapasztalatokat megkövetelő technikai képességek nem igazán skálázhatók, nem lehet hetek, napok vagy akár órák alatt hadkötelezettségek kihirdetésével, szinte a semmiből rutinos IKT rendszermérnököket, üzemeltetőket, informatikai szakértőket előteremteni. Erre a problémára született megoldás lett az Észt Védelmi Liga Kiber Egysége,[93] amely önkéntesek toborzásával igyekszik a szükséges képességhátteret megteremteni ahhoz, hogy az ország informatikai biztonságát jobban szavatolni tudják. A fő célkitűzéseik egyebek mellett a képzett specialisták közötti együttműködés növelése, a kritikus infrastruktúrák kiberbiztonságának növelése, az ehhez szükséges tudás disszeminációjával, a megfelelő kapcsolati hálózatok kiépítése, a képzés és oktatás és a nemzetközi gyakorlatokban való részvétel.

Mikor 2022. február végén Ukrajnát (PwrIndx: 0.3266, 22. helyezés) támadás érte, minden szakértő arra számított, hogy az orosz erők dominanciája a hagyományosnak tekinthető hadviselési módok mellett a hibrid eszköztárba sorolt kiber- és információs műveletekben is látványos lesz. Az azóta eltelt hónapok az első feltételezést sem támasztották alá maradéktalanul, amiben nyilván nagy szerepe volt a jelentős innovációs eredményeket tartalmazó, korszerű nyugati fegyvereknek is – lásd Javelin, HIMARS és a korszerű dróntechnológiák. Az viszont valóban meglepő volt, hogy a korábban már többször és jellemzően nem attribulált módon bizonyító orosz kibererők korántsem hajtottak végre olyan bénító csapásokat, mint amelyre számítani lehetett – talán éppen ennek az előre láthatóságnak is köszönhetően. Igaz, hogy az ukránok nemcsak hadianyagban, kiképzésben és hírszerzési vonatkozásokban kapnak támogatást, de tudható, hogy kibertémákban is folyamatos a konzultáció a védekezés sikerességének növelése érdekében.[94]

Mikhailo Fedorov, az ukrán miniszterelnök-helyettes és digitalizációért felelős miniszter által „IT Army of Ukraine"-nek nevezett formációról beszélve márciusban elmondta[95], hogy az ezen a néven futó Telegram-csatornán már 270 000 tag van. Az ő önkéntes segítségükkel, hacktivista tevékenységgel, az orosz dezinformáció és propaganda ellen küzdenek, és a saját információs műveleteiket támogatják. Időnként már az alapszintű DDOS-támadásokon túlmutatóan már komplexebb ki-

[93] Estonian Defence League's Cyber Unit (https://www.kaitseliit.ee/en/cyber-unit).

[94] Ukraine to be accepted as a Contributing Participant to NATO CCDCOE. *Visit Ukraine. today.* 2022 (https://visitukraine.today/blog/153/ukraine-to-be-accepted-as-a-contributing-participant-to-nato-ccdcoe).

[95] Twitter is part of our war effort – Ukraine minister. *BBC News.* 2022 (https://www.bbc.com/news/technology-60608222).

berműveleteket is végrehajtanak, ami egyre aktuálisabbá teszi azokat a kérdéseket, hogy valós szervezeti keretek nélkül a tevékenységük kinek tudható be, a végrehajtásban részt vevők jogi státuszát (polgári személy-partizán-kombattáns) pedig milyen szabályok mentén kell esetleg megítélni.[96]

3. VÁRHATÓ JÖVŐBELI KÉPESSÉGFEJLESZTÉSI IRÁNYOK ÉS EZEK JOGI KONZEKVENCIÁI

A globálisan és a nemzeteket egyenként is akadályok elé állító eshetőleges, valószínűsíthető vagy akár biztosra vehető körülmények hosszasan sorolhatók. A társadalmi (elöregedő társadalmak, túlzott urbanizáció, népességszám-csökkenés, a kulturális diverzitás egyensúlyhelyzetének megtartása vagy helyreállítása), a technológiai (polgári és a kettős felhasználású termékek sorsa, kiberbiztonsági sebezhetőség, a technológia demokratizálódása), a gazdasági (az EU gazdasági kohéziójának megtorpanása, elmozduló gazdasági erőterek, a jóléti társadalom fenntarthatóságának dilemmája) és a környezeti (éghajlatváltozás, a mezőgazdaság helyzete, világjárványok) és a katonai (a háború egyetemes és időtlen jellege, a béke és a háború közötti határ elhalványulása, a hagyományos és nem hagyományos hadviselés halmazainak összeolvadása, a nem állami szereplők problematikája) veszélyek sok esetben már aktív vagy időzítettnek látszó fordulópontokat hoznak.[97]

Szintén elmondható, hogy habár számos ágazat különíthető el a kérdéskörben, az érintettek körében hiábavaló a megkülönböztetés. Az egyes nemzetek katonai és nemzetbiztonsági képességfejlesztései a terjedelmi keretekre nézve a teljesen kimerítő ismertetést nem tűzte ki célul, de arra mindenképpen alkalmas, hogy szemléltesse a nemzetközi békét és biztonságot fenyegető kihívások átalakulásából és a bevezetésben már említett, az unipoláris világrend idejére tehető világbéke eufóriájából már nem is olyan észrevétlenül felhalmozódott lépéshátrányt. Az európai közösség emellett azzal is kénytelen szembesülni, hogy az átalakuló, hibrid és aszimmetrikus karakterisztikájú hadviselés, habár új tereket nyit a modern hadviselés számos aspektusában, az orosz–ukrán konfliktus régóta elképzelhetetlen, elrettentő például szolgált a reguláris fegyveres konfliktusok világából.

A képességfejlesztésben látható, hogy mindenhol nőtt a kiadások fókuszában a fegyverimport, de ugyanakkor az új területek megjelenése és alapvetően az innováció okán is kiberképességek, a kommunikáció eszközök és módszerek térnyerése is

[96] Lásd Ann Väljataga: *Cyber vigilantism in support of Ukraine: a legal analysis.* Tallinn, CCDCOE, 2022.

[97] European Defence Agency: Exploring Europe's capability requirements for 2035 and beyond (https://eda.europa.eu/docs/default-source/brochures/cdp-brochure---exploring-europe-s-capability-requirements-for-2035-and-beyond.pdf).

megfigyelhető. Mindezekben pedig a tisztán katonai megközelítés önmagában meghaladott és elégtelen, hiszen jól tapasztalhatóan a technikai és a humán hatékonyságnak tendenciózusan érdemi záloga a nemzetbiztonsági szolgálatok bevonása, úgy, a szakmai támogatás, mind az irányítás oldaláról.

A további fejlesztési irányok nagyban prognosztizáltak, ugyanakkor a köztük lévő rangsorolás ahogy napjainkban, úgy a jövőben is szükségtelen, tekintettel arra, hogy az egyes területek kölcsönhatása mára generális. A terrorizmus és a szervezett bűnözés elleni küzdelemben, tekintettel arra, hogy ezek a kihívások gyakorta társulhatnak békeműveleti, határvédelmi katonai feladatokkal, figyelemre méltó az Európai Unió mesterségesintelligencia-alapú arcfelismerő rendszereket érintő rendelettervezete, amellyel kapcsolatban a technikai feltételek már nem, de az alapjogi dilemmák feloldása, a kellő garanciák megteremtése még feladatot jelent.[98] Globálisan kihívást jelent a bűnüldöző, a terrorelhárító szervek és a nemzetbiztonsági szolgálatok közötti információcsere „aranyközepének" megtalálása, ami a feladatrendszerekben lévő keresztmetszetet kiszolgálja, de egyúttal nem jelent információvédelmi csorbát vagy egy-egy szerv képességeinek a minimum középtávon károkat okozó erodálását.[99]

A technológia irányából nézve a dezinformációs hadviseléshez optimális feltételek folyamatos erősödése[100], a felforgató technológiák[101], az autonóm fegyverrendszerek alkalmazási kérdései[102], valamint alapvetően a konfliktusok digitalizálódása olyan folyamatokat jelentenek, amelyek esetében a jogtudomány is csak gyerekcipőben jár.

A humanitárius jog egyes hiányosságai, dilemmái (az egyezményben tiltott kazettás lőszerek használata, aminek Oroszország nem részese, jurisdikciós kérdések a háborús bűncselekmények miatt, az orosz agresszió értékelése és a nki közösség tényleges tehetetlensége, a háború hatása egyes szabadságjogokra (gazdasági szankciók, vállalkozások szabadsága, vagyonelkobzások, média cenzúrázása, az egyes gázszállítási projektek és más hosszú távú együttműködések befagyása és megszűnése).

Jól körvonalazódnak ugyanakkor a már jó ideje feloldásra váró kérdések. Miként fognak a humanitárius jog egyes hiányosságai, dilemmái válaszokra lelni? El-

[98] Ennek kapcsán lásd Koi Tamás: Két uniós adatvédelmi intézmény is tiltaná az arcfelismerést. *HWSW.hu,* 2021 (https://www.hwsw.hu/hirek/63427/europai-unio-bizottsag-mi-ai-rendelet-javaslat-edpb-edps.html).

[99] Cortney Weinbaum – Bradley Knopp – Kim Soo – Yuliya Shokh: *Options for Strengthening All-Source Intelligence: Substantive Change Is Within Reach.* RAND Corporation, RR-A1245-1, 2022 (https://www.rand.org/pubs/research_reports/RRA1245-1.html).

[100] Farkas Ádám – Spitzer Jenő: Az információs korszak és az állami rezíliencia egyes kérdései. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok*, 2021/18. szám, 1–27. o.

[101] Kovács Zoltán – Gurály Roland: A mesterséges intelligencia és egyéb felforgató technológiák hatásainak vizsgálata. *Felderítő Szemle*, 2021/2. szám, 47–62. o

[102] Lásd pl. Schubert Bálint: Az autonóm fegyverrendszerekkel szemben támasztott követelmények a humanitárius nemzetközi jog tükrében. *Honvédségi Szemle,* 2022/3. szám, 20–30. o.

érkezik-e a fegyvereket tilalmazó egyezményekhez csatlakozó államok egysége?[103] A háborús bűncselekmények kapcsán a felelősségre vonhatósághoz teremtődik-e a nemzetközi közösségnek gyakorlati értelemben is vett, kikényszerítő erővel társuló joghatósága? Mit kezd a jogtudomány a háborúnak az egyes szabadságjogokra gyakorolt hatásaival, amelyek többek között a gazdasági szankciók (vállalkozások szabadsága, vagyonelkobzások, hatósági megszorítások) és a médiatartalmak koordinálása után futó cenzúraszabályok következményei? Miként vizsgázik a nemzetközi béke és biztonság letéteményese, a nemzetközi közösség és a mögötte álló nemzetközi jog, a normatív keretek, a bi- és multilaterális egyezmények, szokásjogi keretek?

[103] Példaként említhető, hogy habár 2008 óta él a Kazettás Lőszerekről szóló Egyezmény, Oroszország az ukrán konfliktusban is alkalmaz ilyen eszközöket. Lásd HRW: Oroszország kazettás bombákat használ Ukrajnában, amelyek súlyos károkat okoznak a civileknek. *Szabad Európa,* 2022 (https://www.szabadeuropa.hu/a/hrw-oroszorszag-kazettas-bombakat-hasznal-ukrajnaban-amelyek-sulyos-karokat-okoznak-a-civileknek/32003930.html).

HÓDOS LÁSZLÓ

A kibertér és a mesterséges intelligencia jelentősége és kihívásai a jogállamok nemzetbiztonsági feladatellátásában

1. A TÉMAVÁLASZTÁS AKTUALITÁSA, INFORMÁCIÓFÚZIÓ, ADATANALITIKA, MESTERSÉGES INTELLIGENCIA

A nemzetbiztonsági szolgálatok által alkalmazott erők, eszközök és módszerek együttes hatásmechanizmusának szabályozási eszközrendszere a jogforrási hierarchia legmagasabb szintjétől a legalacsonyabbig terjedő széles spektrumot ölel fel. Ezek a magyar nemzet biztonságának védelme érdekében – döntően titokban, néha nyíltan – kerülnek alkalmazásra a szolgálatok munkatársai által. A jogi normákban megjelenő feladatok végrehajtása esetenként alapjog-korlátozással jár együtt, emiatt ezeket az állami monopóliumként kodifikált tevékenységeket szigorú előírások között gyakorolhatják az erre feljogosított szervezetek.

A normaalkotás ezeken a területeken sokkal összetettebb, mint pusztán kodifikációs feladat, mivel a történelmi előzményeket, a 21. századi biztonsági kihívásokat és a jogalkotási rendszer aktuális lehetőségeit egyaránt figyelembe kell venni. Megítélésem szerint mindhárom szempontrendszernek megfelelő szakmai koncepciót, stratégiát és ennek alapján kialakítandó jogi normákat szükséges készíteni, és új megoldásokat alkalmazni. Ilyen új, a 21. századi kihívásokra reagáló jogalkotási és szakmai megoldás volt 2012. január 1-jén a Katonai Nemzetbiztonsági Szolgálat létrehozása is.

Az integráció szükségességével összefüggésben nem szabad megfeledkezni arról, hogy *„…a globális biztonsági környezetben zajló változások következtében felértékelődik a hírszerzés es az elhárítás szerepe. A műveleti területre jellemző összetett kihívások, valamint a gyakran változó biztonsági helyzet szintén megnöveli a pontos és időbeni információk és értékelések iránti igényt”*.[1]

A 2012. május 24-én a Nemzeti Közszolgálati Egyetemen megrendezett „Nemzetbiztonsági kihívások, nemzetbiztonsági szolgálatok” című szakmai-tudományos konferencián Kovács József altábornagy A Katonai Nemzetbiztonsági Szolgálat az egyesítés után című előadásában elmondta, hogy *„az integrációval a kormányzat célja volt, hogy egy szakmailag eredményesebb, költségvetését tekintve pedig takarékо-*

[1] Szentgáli Gergely: Csendben szolgálni: 1. rész: A magyar nemzetbiztonsági szektor helyzete és átalakítása 2010 es 2014 között. *Hadtudomány*, 2015/1-2. szám, 52. o.

sabb szolgálat jöjjön létre, ahol jobban biztosítható a hírszerző és elhárító tevékenységből származó információk áramlása, megszűnnek a párhuzamosságok és növekszik az állomány felkészültsége. További cél, hogy a két szakterület együttműködésének szorosabbra fűzésével még eredményesebbé váljon a hadműveleti területeken szolgáló magyar kontingensek hírszerző és biztonságvédelmi támogatása."[2]

A katonai szolgálatok integrációval összefüggésben megfogalmazott kormányzati törekvések látszólag megvalósultak, a nemzetbiztonsági szolgálatok rendszerének a jelenlegi struktúráját megvalósító átalakítása – a Terrorelhárítási Információs és Bűnügyi Elemző Központ[3] – létrehozásával, illetve 2022 első félévben lezajlott jelentős hatáskör bővítésével (és átnevezésével) befejezettnek látszik, azonban a titkos információgyűjtés széles spektrumán működő polgári szolgálatok tevékenységének összehangolására, illetve a szorosabb szervezeti együttműködésére továbbra is jelentős igény mutatkozik. A polgári szolgálatok egyes szerveinek esetleges integrációja mind ez idáig várat magára, azonban ennek megvalósulása előtt jogalkotói akadály nincs. Nyilván ebben az esetben az ágazatok szakmai tevékenysége közötti redundancia biztosításának fontossága elhanyagolhatatlanná válik.

Ugyanakkor álláspontom szerint ezen szakági normák és struktúrák jelenleg csak korlátozott hatékonysággal képesek működni, mert a történelmi távlatból még csak részben vizsgálható 20. század végén, illetve 21. század elején keletkezett tapasztalatokat minden részletre kiterjedően még nem sikerült rendszerezni, értékelni és a jogalkotás szintjén hasznosítani. Ezen nemzetbiztonsági értelemben vett szakmai, valamint hagyományos értelemben vett történelmi és jogi ismeretek, valamint az ezekkel összefüggésben feltárt események, adatok, egymásra gyakorolt hatásuk feldolgozásából nyerhető eredményeket a jogszabályokban, a közjogi szervezetszabályozó eszközökben és ezek alapján a belső rendelkezésekben is hasznosítani szükséges.

A kutatás során a nemzetbiztonsági szolgálatok vonatkozásában a 20. század és a 21. század – jog-, illetve szakmatörténeti szempontból – releváns helyzeteinek, eseményeinek fókuszba állításával szeretném a fenti, interdiszciplináris szempontrendszer szerinti vizsgálatot végrehajtani, ideértve a témakörben közismert tényeknek és félelmeknek az ismertetését is.

Az ötszolgálatos modell kialakításához hasonló jelentőségű változást okozott nemzetbiztonsági ágazat számára a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény katonai nemzetbiztonsági szolgálatok összevonásával kapcsolatos módosításáról, valamint az azzal összefüggő további törvénymódosításokról szóló 2011. évi CLXXI. törvény kihirdetése[4] és hatálybalépése[5]. A vizsgált időszak kiemel-

[2] Kovács József: A Katonai Nemzetbiztonsági Szolgálat az egyesítés után. *Hadtudomány,* 2013/1–2. szám, 87. o.

[3] 2016. július 17-én lépett hatályba a TIBEK-et létrehozó törvénymódosítás.

[4] 2011. december 14-én.

[5] 2012. január 1-jén.

kedő – a 21. századi kihívásokra reagáló – jogalkotási és szakmai megoldása volt a Katonai Nemzetbiztonsági Szolgálat létrehozása[6] 2012. január 1-jén.

Kiemelkedő jelentőségű, a nemzetbiztonsági szolgálatok adatkezelő, értékelő-elemző és kormányzati tájékoztató tevékenységét érintő, koncepcionális vitát generáló jogszabálytervezetet ismerhetett meg 2011 novemberében az olvasó (szakmai szervezetek és nyílt köröztetés miatt a széles közvélemény egyaránt) az egyes rendvédelmi tárgyú törvények módosításáról, valamint az azzal összefüggő további törvénymódosításokról szóló T/5004. számú törvényjavaslat tanulmányozása során. Urbán Attila foglalja össze a javaslat sorsát, miszerint *„a Nemzeti Információs és Bűnügyi Elemző Központ létrehozását célzó javaslat kapcsán a parlamenti vitában, illetve a közéleti nyilvánosság fórumain – a szervezet adatbázisokhoz való közvetlen hozzáférése és adatkezelési jogosultságai kapcsán megfogalmazott alapjogi dilemmák mellett – ismét felbukkantak a szolgálatok független elemző-értékelő és döntéshozókat közvetlenül elérő tájékoztató tevékenységét, illetve a szektoriális tárcaálláspontokat preferáló megközelítések. Jellemzően ez utóbbi szempontok jelentek meg azokban kormánypárti képviselők (köztük a polgári nemzetbiztonsági szolgálatokat korábban irányító házelnök) által benyújtott módosító javaslatokban*[7]*, amelyeket az Országgyűlés többsége a BM eredeti előterjesztésével szemben támogatott."*[8]

A koncepció így akkor nem vált valóra, ugyanakkor a tervezetben megjelenített szakmai célok indokoltságát és szükségességét alátámasztja,[9] hogy 2018 óta a polgá-

[6] A 2012 és 2020 közötti időszak fontos eseményeit és a jövőre vonatkozó elképzeléseket lásd Kenedli Tamás: A Katonai Nemzetbiztonsági Szolgálat szakmai fejlődésének legfontosabb sajátosságai az elmúlt években. *Nemzetbiztonsági Szemle*, 2020/1. szám, 74–94. o.

[7] Kövér László házelnök módosító javaslata a törvénytervezethez. 2011. november 30. (www.parlament.hu/ irom39/05004/05004-0022.pdf).

[8] Urbán Attila: A koordinációs folyamatok intézményi hátterének evolúciója a magyar nemzetbiztonsági igazgatásban. *Nemzetbiztonsági Szemle*, 2020/1. szám, 24. o.

[9] Ezen kiemelkedően fontos, információfúziós célok az Nbtv. Indokolásában olvashatók: *A TIBEK feladatai közül kiemelésre érdemes az együttműködő, mindenekelőtt a nyomozó és a nemzetbiztonsági szervek működésbeli párhuzamosságainak a kiszűrése. Mind a terrorelhárítás, mind az állami büntetőigény érvényesítése, mind a szuverenitás érdekében végzett titkosszolgálati tevékenység területén rendkívüli kockázatokkal járnak a párhuzamos nyomozások, illetve a párhuzamos titkos információgyűjtések. Ezek kiszűrése és jelzése a megfelelő együttműködő szerveknek a TIBEK fontos feladata. Ezzel a TIBEK nagymértékben elősegíti a terrorcselekmények megelőzését, a nyomozások eredményességét, illetve az adattakarékosság alkotmányos elvének érvényre juttatását. A TIBEK az együttműködő szervek számára folyamatosan továbbítja a hatáskörükbe tartozó adatokat, ezzel egyidejűleg javaslatot tesz az együttműködő szervek számára az adatok mikénti felhasználására. A TIBEK mint információfúziós központ rendkívül hatékony segítséget nyújthat a TEK terrormegelőző, terrorelhárító tevékenységéhez mivel a rendelkezésére álló adatokból hatékony következtetést tud levonni a terrorszervezetek magyarországi tevékenységéről, a terroristák megjelenéséről és a PNR adatok alapján mozgásukról. A TIBEK koordinációs tevékenysége során figyelemmel kíséri, hogy nem áll-e rendelkezésre az általa átadott adattal kapcsolatos pontosító vagy kiegészítő adat: amennyiben igen, a TIBEK a feladatkörében észlelt kapcsolódó adatot átadhatja az adat felhasználására hatáskörrel rendelkező együttműködő szervnek. A TIBEK fontos feladatokat lát el a szervezett bűnözés elleni küzdelemben és az illegális vagyonok felderítésében is. A TIBEK*

ri hírszerzésért felelős Információs Hivatal és a Katonai Nemzetbiztonsági Szolgálat – önálló elemző-értékelő képességeit, valamint a döntéshozók közvetlen tájékoztatásának közvetlen lehetőségét megőrizve, eseteként a 2016-ban létrehozott információfúziós központtól független formában – közvetlenül elégíti ki a kormányzati hírigényt. A gazdaságosságot és a gyors információáramlást célul kitűzve ezt a funkciót megerősítve és kiegészítve a 2022 nyarán Nemzeti Információs Központtá átnevezett fúziós központ infrastruktúráján keresztül zajlik a hírigények vétele és kielégítése, azonban a nemzetbiztonsági információk áramlásának nyomon követését továbbra is Nemzeti Információs Államtitkárság végzi. A mesterséges intelligencia által elvégezhető adatanalitika természetesen az információfúziós központok működésére is jelentős hatást gyakorolhat, hiszen számos álláshely veszélybe fog kerülni, valamint jelentős kapacitáskoncentráció valósítható meg az új informatikai fejlesztéseknek köszönhetően, ami minden olyan tevékenységet ki tud váltani majd, amelyhez kizárólagos humán kognitív képességek nem szükségesek. Mivel a fejlesztők nemzetbiztonsági szakági ismeretekkel korlátozottan rendelkeznek, ezért az adatfeldolgozás, illetve az analitika területén valósulhat meg leginkább a mesterséges intelligencia megjelenése a rendvédelmi, illetve nemzetbiztonsági feladatellátás során.

Megítélésem szerint központosított, egycsatornás hírigény-kielégítés a jelenlegi, elsősorban katonai jellegű, illetve hátterű biztonsági kihívások időszakában elsődlegesen adminisztratív támogatást jelent a Katonai Nemzetbiztonsági Szolgálat számára a Nemzeti Információs Központ részéről. A folyamatban lévő ágazati reform idején különösen fontos megjegyezni, hogy a redundancia megőrzése (polgári és katonai ágazat között) talán sosem volt ennyire indokolt.

2. A PROAKTÍV SZEMLÉLETMÓD MEGJELENÉSE A SZAKMAI JAVASLATOK JOGI MEGVALÓSÍTÁSA SORÁN

Igaz, hogy már 2012. január 1-jétől[10] – a kibertérből érkező fenyegetésekkel összefüggő cselekvési kényszer[11] hatására – a jogalkotó a Katonai Nemzetbiztonsági

a terrorszervezetekkel, illetve a konkrét terrorcselekményekkel kapcsolatos adatait soron kívül továbbítja a TEK részére.

[10] Kenedli Tamás – Kis-Benedek József – Szabó Károly: A katonai felderítés és elhárítás evolúciója, szervezete és feladatkörei. In Farkas Ádám – Kádár Pál (szerk.): *Magyarország katonai védelmének közjogi alapjai.* Budapest, HM Zrínyi Térképészeti és Kommunikációs Szolgáltató Közhasznú Nonprofit Kft, 2016, 123. o.

[11] A kibertér és az információ fegyverként értelmezése kapcsán például lásd Simon László – Magyar Sándor: A terrorizmus és indirekt hatása a kiberterében. *Szakmai Szemle*, 2017/3. szám, 89–101. o.; Simon László – Magyar Sándor: A terrorizmus és indirekt hadviselése az EU kiberterében. *Szakmai Szemle*, 2017/4. szám, 57–68. o.; Simon László: Az információ mint fegyver? *Szakmai Szemle*, 2016/2. szám, 34–60. o.; Kelemen Roland – Pataki Márta: Kiberterrorizmus: A terrorizmus új arca. *Magyar Rendészet*, 2014/5. szám, 103–116. o. Kelemen Roland – Pataki Márta: A kibertámadások nemzetközi

Szolgálat feladatává tette a honvédelmi érdeket veszélyeztető kibertevékenységről történő információgyűjtést, de e tekintetben fajsúlyos változást az Nbtv. 6. § g) pontjának evolúciója hozott. Ez ugyanis tükre annak, hogy miként reagált a jogalkotó a területen folyamatosan megnyilvánuló, helyesebben folyamatosan változó kihívásokra. A publikáció készítésekor hatályos, de módosítás alatt álló normaszöveg feladatok oldalán tapasztalható bővülése, miszerint a Katonai Nemzetbiztonsági Szolgálat *„információkat gyűjt a honvédelmi érdeket veszélyeztető kibertevékenységekről és -szervezetekről, jogszabály keretei között ellátja a honvédelmi ágazat elektronikus információbiztonsági feladatait, biztosítja a honvédelemért felelős miniszter által vezetett minisztérium, valamint a Magyar Honvédség Parancsnoksága információvédelmi tervező munkájához szükséges információkat, továbbá kibertér műveleti képességeivel ellátja a honvédelmi érdekek nemzetbiztonsági jellegű védelmét és a Magyar Honvédség kibervédelmének és műveleteinek támogatását"* fejezi ki a leginkább, hogy mennyivel bonyolultabbá vált mindössze néhány év alatt ennek az egy feladatnak a jogi absztrahációt követő megjelenítése a törvényi tényállásban. Az elmúlt években, különösen 2019-ben és 2020-ban tapasztalható körülmények felhívták rá a figyelmet, hogy a kibertérben jelen lévő, pontosabban onnan érkező, azt felhasználó dezinformációs művelet a járvány idején (de minden más, különleges jogrend kihirdetését megalapozó helyzetben) jelentősebb eredménnyel jár (hátránnyal fenyeget). Ez szorosan összefügg a kibertér kihívásainak társadalmi-politikai vonatkozásaival, illetve az ezekkel szembeni fellépés komplex védelmi rendszerre gyakorolt kihívásaival. Emiatt komolyabb dologi és személyi erőforrásokat igénylő feladatokat képez a nemzetbiztonsági elhárításért és rendvédelemért felelős szervek számára is, így erre a (veszélyek elhárítására történő) folyamatos felkészülés, illetve a (jövőbeli, konkrét) feladatok tervezése során a nemzetbiztonsági szolgálatoknak és más állami szerveknek. Emiatt kell különös figyelmet fordítani az öntanuló ellenfelekkel szembeni hadviselésre való felkészülésre.,

---

jogi értékelése. *Katonai Jogi és Hadijogi Szemle*, 2015/1. szám, 53–90. o.; Kelemen, Roland: Cyber Attacks and Cyber Intelligence in the System of Cyber Warfare. In Szabó Miklós (szerk.): *Doktoranduszok Fóruma Miskolc 2016. november 17. Állam- és Jogtudományi Kar szekciókiadványa.* Miskolc, Miskolci Egyetem, 2017, 117–122. o.; Kelemen Roland – Simon László: A kibertérben megjelenő fenyegetések és kihívások kezelésének egyes nemzetközi jogi problémái. In Farkas Ádám – Végh Károly (szerk.): *Új típusú hadviselés a 21. század második évtizedében és azon túl – intézményi és jogi kihívások.* Budapest, Zrínyi Kiadó, 2020, 150–170. o.; Kelemen Roland – Farkas Ádám: To the Margin of the Theory of a New Type of Warfare: Examining Certain Aspects of Cyber Warfare. In Szabó Marcel – Gyeney Laura – Láncos Petra Lea (szerk.): *Hungarian Yearbook of International law and European Law (2019).* Den Haag, Eleven International Publishing, 2020, 203–226. o.

3. HIBRID HADVISELÉS ÉS KIBERVÉDELEM

A hibrid és kiberhadviselés közötti kapcsolat összefüggései jól láthatók.[12] Hogyan kapcsolódik előbbi kettőhöz „a lakosság tömeges és súlyos megbetegedésének kockázatát hordozó járványos betegség magyarországi megjelenése és gyors terjedése?". Lehetséges-e előzőek káros hatásainak szándékos, gondatlan vagy vétlen növelése a járvány miatt elrendelt veszélyhelyzet idején? Elegendő a kormányzati tájékoztatást követnünk ahhoz, hogy felismerjük, a kibertérben elindított dezinformáció, mint az országos nyilvánosságot kapott „Budapestet hamarosan le fogják zárni" tartalmú hamis híresztelés miféle politikai, gazdasági, társadalmi károkat képes okozni.

A Készenléti Rendőrség Nemzeti Nyomozóiroda és a Nemzetbiztonsági Szakszolgálat gyors, határozott intézkedéseinek köszönhetően a Budapest lezárásáról szóló, de más álhírek terjesztőit is azonosították, és velük szemben büntetőeljárás indult. A bármely okból kialakult sebezhetőség kiváló lehetőség az online csalások elkövetői számára is, akik szintén a kibertérben követik el a bűncselekményeket. A sebezhetőség a járvány miatti bizonytalanság eredményeként alakul ki. Ennek legjobb ellenszere a magyar kormány által is alkalmazott széles körű tájékoztatás. Interneten, televízióban, nyomtatott és elektronikus sajtóban közöl folyamatosan adatokat a kormányzat, megerősíti a társadalomban, hogy a helyén van az államapparátus, pánikra nincs ok. A dezinformáció terjesztése, a bizalom aláásásának kiváló eszköze ellen csak így lehet felvenni a harcot. Azok a biztonsági kockázatok, amelyeket sajátos szempontok szerint kiemeltem, pontosan a társadalom kötőszövetét rombolják le. Az államapparátus vagy a helyi szintű vezetők munkájába vetett bizalmat, de akár a kormányzati vagy nem kormányzati munkahelyek légkörét is teljesen tönkre tudják tenni azok a megnyilvánulások, melyeket jobb esetben csak sajtóhírekből ismertünk meg az elmúlt hónapokban.

Az álhírek terjesztésének egyik legveszélyesebb területe a jogalkotás tevékenységének támadása hazai és nemzetközi színtéren. Az úgynevezett lawfare[13], amely

[12] A különleges jogrendet, illetve a kibertérben zajló konfliktusokat érintően konferenciák tekintetében többek között lásd: 2017. április 21. Pázmány Péter Katolikus Egyetem Jog- és Államtudományi Kar, Magyar Tudományos Akadémia Társadalomtudományi Kutatóközpont Jogtudományi Intézet, Magyar Katonai Jogi és Hadijogi Társaság: A különleges jogrend című konferencia, Budapest; 2019. május 8. Széchenyi István Egyetem, Magyar Katonai Jogi és Hadijogi Társaság: Az erőszak tilalmától a kibertérben zajló konfliktusokig című konferencia, Győr; 2019. május 29. Nemzeti Közszolgálati Egyetem, Széchenyi István Egyetem, Magyar Katonai Jogi és Hadijogi Társaság: 80 éves az első magyar honvédelmi törvény című konferencia, Budapest; 2019. november 19. Nemzeti Közszolgálati Egyetem, Magyar Katonai Jogi és Hadijogi Társaság: Honvédelmi jog és igazgatás aktuális kérdései című konferencia, Budapest.

[13] A *„lawfare"* kifejezés használatáról és jelentéséről bővebben lásd Charles J. Dunlap: Law and Military Interventions: Preserving Humanitarian Values in 21st Conflicts. presented at Humanitarian Challenges in Military Interventions Conference (November 29, 2001) (http://people.duke.edu/~pfeaver/dunlap.pdf). A kifejezés először John Carlson – Neville Yeomans: Whither Goeth the Law –

elsősorban a jogi eszközök alkalmazását jelenti a hibrid hadviselés során, megítélésem szerint értelmezhető úgy, hogy idesorolandó a jogalkotás legfelsőbb szintje által alkotott jogforrások folyamatos, az esetek többségében alaptalan támadása is, mivel a célja a jogalkotó hiteltelenítése, a belé vetett közbizalom megingatása. A jog uralmának helyességébe vetett társadalmi bizalom gyengítése alkalmas az állam destabilizálására, mozgásterének csökkentésére. Ezt a lehetőséget pedig fokozni tudják azok a kihívások, amelyek a digitalizáció hozadékai folytán szélesebb értelemben is érintik az állam és jog szisztémáit.

A publikáció készítésekor hatályos magyar Nemzeti Biztonsági Stratégiában[14] (a továbbiakban: NBS) szereplő, a tanulmány fókuszába helyezett kihívások elleni küzdelem során kulcsszerepe van a proaktív jogalkotásnak és a megfelelő alkotmányos kontroll melletti jogalkalmazásnak.[15]

4. A MINDENNAPOKBAN MEGJELENŐ MESTERSÉGES INTELLIGENCIA ÉS EGYES BIZTONSÁGI ASPEKTUSOK

A mesterséges intelligenciáról egyre többet hallunk, a közeljövő meghatározó technológiájának tartják. Lehetővé teszi a technika számára, hogy érzékelje környezetét, kölcsönhatásba kerüljön azzal, amit észlel, problémákat oldjon meg, és konkrét cél elérése érdekében megtervezze a saját lépéseit. A számítógép nemcsak adatokat vételez (már előkészített vagy összegyűjtött adatokat arra alkalmas perifériáin, például kameráján keresztül), hanem fel is dolgozza azokat, és reagál rájuk. Ezek a rendszerek képesek viselkedésük bizonyos fokú módosítására is, a korábbi lépéseik hatásainak elemzésével és önálló munkával. A technológia egyes fajtái már több mint 50 éve léteznek, de a teljesítmény fejlődése, a hatalmas mennyiségű adat feldolgozása és az új algoritmusok az elmúlt években jelentős áttörést jelentettek a területen. Az internetes vásárlásaink és a számunkra küldött célzott, személyre szabott hirdetéseket mutathassanak nekünk online, például böngészési előzményeink és vásárlásaink

---

Humanity or Barbarity, a The Way Out – Radical Alternatives in Australia. In M. Smith – D. Crossley (szerk.): *Lansdowne.* Melbourne, 1975. (http://www.laceweb.org.au/whi.htm) műben szerepel, ugyanakkor a kifejezést számos, eltérő jelentéssel használják. A tanulmány szempontjából a Dunlap által alkalmazott megközelítésében használom.

[14] 1163/2020. (IV. 21.) Korm. határozat – Magyarország Nemzeti Biztonsági Stratégiájáról

[15] Az NBS kifejezetten előírja, hogy a biztonság egyes részterületeiért felelős állami szervezeteknek a Stratégiában megfogalmazott iránymutatásokkal összhangban kell megalkotniuk és felülvizsgálniuk a tevékenységükre vonatkozó szakági szabályzókat, különös tekintettel a nemzeti katonai, a rendészeti, a nemzetbiztonsági, a terrorelhárítási, a katasztrófavédelmi, a kiberbiztonsági és a migrációs területekre. Mindezt úgy kell elvégezni, hogy a hatályos NBS rendelkezéseit is a korábban említett, folyamatos felülvizsgálati kötelezettség terheli, így amennyiben valamely érintett szerv hatáskörében erre okot adó körülményt derít fel, jeleznie szükséges azt az irányító tárc(áj)a felé, hogy a szükséges normaalkotás kezdeményezhetővé váljon.

vagy más internetes tevékenységünk alapján. A mesterséges intelligencia rendkívül fontos az internetes kereskedelemben például a termékek optimalizálása vagy a készletek és a logisztika megtervezése miatt, vagyis a gazdasági társaságok számára konkrét értékkel bír minden, a felhasználó szokásairól szóló információ.

Ezek az információk eladhatók, a felhasználó ingyen vagy egy nyereményjáték keretében (odaadott vagy) megadott adatait harmadik fél számára értékesíti számos adatkezelő. Az internetes böngészés természetesen hasznos is másik oldalról nézve, hiszen a böngészők mögötti keresőmotorok a felhasználók által rendelkezésre bocsátott rendkívül nagy mennyiségű adatot kiértékelik, majd szokásainkból tanulnak. Ezt követően pedig csakugyan olyan találatokat kapunk egy-egy kereséskor, amelyek számunkra relevánsak. Nyilván az ár-érték arányt alapul véve, figyelemmel arra, hogy ezeket az adatokat jó esetben anonimizáltan, kevésbé jó esetben névvel, (szállítási)címmel, (értesítési) telefonszámmal együtt adja el valamelyik szoftveróriás, harmadik félnek, érdemes úgy tekintenünk virtuális életünkre, mint egy sokak által hozzáférhető, nyitott könyvre… Az öntanuló szoftverek korában az online meetingekre berendelő alkalmazások világában a személyi asszisztens is alkalmazások egyvelege, sok esetben már komplex vagy egymással összehangolt szoftverek váltják ki a humánerőforrást. Előbbiek használata vélhetően számos álláshely megszűnését is magával hozza. Bár a mesterséges intelligencia várhatóan jobb munkahelyeket is teremt, az oktatásnak és a képzésnek döntő szerep jut majd abban, hogy képzett munkaerőt biztosítson a területen. Nyilván a mesterséges intelligencia számos élethelyzetet és azokra adott több ezer vagy több száz éve társadalom által elfogadott intézményt egy másodperc törtrésze alatt fog a történelem szemétdombjára vetni, remélhetőleg az emberiséget, mint a legkárosabb állatfajt, majd csak később igyekszik „drasztikusan megjavítani". Az emberrel fizikai kapcsolatban álló alkalmazások is jelenthetnek fizikai veszélyt, ha azokat nem megfelelő gondossággal tervezik vagy alkotják meg, vagy ha a szoftvert feltörik, illetve az adatokkal visszaélnek.

Az okoseszközök a mesterséges intelligencia használatával a lehető legrelevánsabb és személyre szabottabb termékeket kínálják, jelzik, hogy elfogyott az adott élelmiszer, vagy a papír a nyomtatóból, különösen, ha ezek összeköttetésben is vannak. A virtuális asszisztensek válaszolnak a kérdéseinkre, és segítenek a napi rutin megszervezésében, különösen úgy, hogy a navigáció is legtöbbször a mesterséges intelligenciát használja, ahogyan az okos termosztátok energiát takarítanak meg, míg az intelligens városok fejlesztői azt remélik, hogy szabályozhatják a forgalmat a dugók csökkentése érdekében. A fordító szoftver, akár írott, akár szóban elmondott szövegen alapul, a mesterséges intelligenciára támaszkodik a fordítások biztosítása és fejlesztése érdekében, hasonlóan az automatikus feliratozáshoz. A mesterséges intelligenciát használó rendszerekkel összefüggésben azonban feltétlenül tisztázandó, hogy ki a felelős a mesterséges intelligenciával működtetett eszköz vagy szolgáltatás által okozott károkért. Számos olyan esetről olvashattunk az elmúlt években a különböző médiafelületeken, hogy önvezető autó okozott balesetet, kárt, halálesetet.

Felmerül a kérdés, hogy ilyen esetekben kinek kell helytállnia? A tulajdonosnak, az autógyártónak vagy a programozónak kell majd a felelősséget vállalnia? Hogyan értékeli majd a polgári és büntetőjog ezeket a kérdéseket[16]? Ha a robot vagy drón vagy autógyártó nem vonható felelősségre, akkor az csökkentheti az emberek bizalmát a – jelen tanulmányban konkrétan meg nem nevezendő – piacvezető márka, illetve az egész technológia iránt. Tudja-e a jogalkotás ezeket a helyzeteket proaktívan kezelni, és miként lehet majd az így alkotott szabályokat úgy átültetni a gyakorlatba, hogy az ne lehetetlenítse el az innovációt[17]?

A bíróság számára egy megalapozott indokolás kialakításához nélkülözhetetlen a vonatkozó jogi normák, az esetjog és a jogi irodalom egyidejű magas szintű ismerete. Ennek okán valamennyi bírói döntést hosszú és aprólékos kutatásnak szükséges megelőznie.[18]

A jogi kutatószoftverek *(legal research softwares)* ezt a tevékenységet gyorsítják fel. Rendszeresen frissülő adatbázisaikban kulcsinformációk megadásával az összes elérhető releváns adatot egy keresési eredményben összegzi a program.[19]

Ahogyan tanulmányában Kálmán Kinga kiemeli,[20] *„a tengerentúlon az egyik, ha nem a legelterjedtebb ilyen jogi kutatószoftver a LexisNexis. Adatbázisa több, mint 83 milliárd jogszabályt és bírói esetjogot, 40 ezer jogi folyóiratcikket és 700 millió cégnyilvántartási adatot tartalmaz. Az alkalmazás megerősítésként értékeli, ha a felhasználó rákattint a keresési eredményre, a »linkelt oldalon töltött idő« hosszát, valamint azt,*

[16] A kérdés vizsgálata során érdemes áttanulmányozni: Kálmán Kinga: Nyomokban kódokat tartalmazhat? A mesterséges intelligencia igazságszolgáltatásban történő alkalmazásának alkotmányjogi vonatkozásai a tisztességes eljáráshoz való jog tükrében (https://jog.tk.hu/mtalwp/nyomokban-kodokat-tartalmazhat-a-mesterseges-intelligencia-igazsagszolgaltatasban-torteno-alkalmazasanak-alkotmanyjogi-vonatkozasai-a-tisztesseges-eljarashoz-valo-jog-tukreben), valamint Richard Sussking: *Online Courts and the Future of Justice.* Oxford, Oxford University Press, 2019.

[17] A témával összefüggésben lásd Kecskés Gábor: Az autonóm járművek jogi kérdéseinek nemzetközi kontextusa, különös tekintettel a környezetjogi vetületekre. *Állam- és Jogtudomány,* 2020/4. szám, 52–64. o.; Mezei Kitti: A modern technológiák kihívásai a büntetőjogban, különös tekintettel a kiberbűnözésre. *Állam- és Jogtudomány*, 2020/4. szám, 65–81. o.; Rácz Lilla: A személy és a dolog fogalmának (lehetséges) változásai a mesterséges intelligencia és a kriptovaluták világában. *Állam- és Jogtudomány*, 2020/4. szám, 82–107. o.

[18] Brazil Fellebbviteli Bíróság 2018–2019. év 1. beszámoló. (https://www.stj.jus.br/sites/portalp/SiteAssets/documentos/noticias/Relat%C3%B3rio%20de%20gest%C3%A3o.pdf.).

[19] Jogi kutatószoftverek működése a gyakorlatban: NORTHPOINTE SUITE: Practicioners's Guide to COMPAS Core. (https://assets.documentcloud.org/documents/2840784/Practitioner-s-Guide-to-COMPAS-Core.pdf). Olivia Mivill: Malaysian judiciary makes history, uses AI in sentencing. *New Straits Times,* 2020. (https://www.nst.com.my/news/nation/2020/02/567024/malaysian-judiciary-makes-history-uses-ai-sentencing).

[20] Kálmán Kinga: Nyomokban kódokat tartalmazhat? A mesterséges intelligencia igazságszolgáltatásban történő alkalmazásának alkotmányjogi vonatkozásai a tisztességes eljáráshoz való jog tükrében. *MTA Law Working Papers,* 2021/2. szám.

ha a felhasználó elmenti a találatot. Ez alapján javítja az adatbázisát a minél relevánsabb keresési eredmények elérése érdekében."

Az egyik legismertebb online bíróság Kínában található: Hangzhou városában 2017-ben állították fel az első internetbíróságot. Kínában, amely a világon a legtöbb, mintegy 850 millió mobilinternet-felhasználóval rendelkezik, a digitalizálási erőfeszítések részben azt a célt szolgálják, hogy a bíróságok lépést tarthassanak a mobilfizetés és az e-kereskedelem által generált növekvő ügyteherrel. A hivatalos kínai adatok szerint a Legfelsőbb Népbírósággal közösen összesen 118 764 keresetet fogadtak be, és 88 401-et zártak le, és összesen közel hárommillió üggyel foglalkoztak. Ni Defengneknek, az internetbíróság alelnökének álláspontja szerint a késedelem az igazságszolgáltatás akadályát képezi, emiatt feltétlenül szükséges felhasználni a digitalizáció minden eszközét az igazságszolgáltatás támogatására. A bíróság eljárását bárki kezdeményezheti digitalizációval kapcsolatos témában (például fogyasztóvédelmi panaszok, szerzői jogi viták az online térben, elektronikus fizetés). Az egész folyamat az online térben folyik, a felek avatarjaikkal megjelenítve videóhívással vehetnek részt a tárgyaláson, illetve az előterjeszteni kívánt bizonyítási indítványukat szintén online, blokklánc-technológiával titkosított formában tudják feltölteni. A bíró személyében mesterséges intelligencia áll velünk szemben, amely a rendelkezésre álló adatok alapján gépi tanulási folyamat eredményeként dönt és szolgálatat igazságot.



Az interneten elérhető bemutatóban[21] a Kína nemzeti jelképe alatt ülő fekete köpenyes virtuális bírótól elhangzó „Van-e az alperesnek kifogása a felperes által benyújtott bírósági blokklánc-bizonyítékok természete ellen?" – kérdésre a tárgyalást megelőző ülésen a „Nincs kifogás" – válasz érkezett az emberi felperestől. A statisztikai adatokból kimutatható sikerek miatti eufória mellett persze könnyen lehet egy „Nagy testvér mindent lát" érzésünk, és valljuk be, nem is alaptalanul. Minden esetben, akár a bűnelkövető bűnismétlésének várható valószínűségét becsüli meg, akár a kényszerintézkedés legcélszerűbb eszközét sugalmazza a mesterséges intelligencia,[22] fontos megjegyezni, hogy a folyamatos humán kontroll nélkül könnyedén egy utópisztikus világban találjuk magunkat, ahol az öntanuló szoftverek az empátia hiánya, illetve korlátozott volta miatt meglepő javaslatokat tehetnek a jogalkalmazó számára. Persze az sem zárható ki, hogy a mesterséges intelligencia helyes döntést fog hozni annak ellenére is, hogy az emberi résztvevő ezt nem így érzi.

Ha nem kezelik megfelelően, a mesterséges intelligencia téves döntésekhez vezethet, vagy az etnikai hovatartozásra, nemre és életkorra vonatkozó adatokkal befolyásolhatja a döntéseket egy ingatlan bérbeadása vagy akár egy elbocsátás során. Emellett befolyásolhatja a magánélethez és az adatvédelemhez való jogot. Használható például arcfelismerő berendezésekben, vagy online nyomon követés és profilalkotás céljából. A mesterséges intelligencia szerepet játszhat a gyülekezési és tiltakozási szabadság sérelmében is, mivel nyomon követheti a bizonyos eszmékhez vagy egy tüntetéshez kötődő személyeket. Vagyis egy járvánnyal fertőzött területről érkező felhasználó esetében a mesterséges intelligencia jelzi az arra jogosult állami szerv részére, hogy fokozott egészségügyi kockázatot jelenthet a jelenléte, vagy megszegte a karanténszabályokat, de egy meghatározott időben és helyen tartózkodó demonstráló is kiszűrhető, beazonosítható. A helyes állami célkitűzések, mint a terrorelhárítást célzó funkciók is felhasználhatóak ilyen módon egyes csoportok, személyek megfélemlítésére, elnyomására. Emiatt van kiemelkedő jelentősége annak, hogy a humán oldalon milyen célok, szándékok vezérlik a mesterséges intelligenciával bíró fizikai, illetve virtuális eszközöket.

[21] Az ismertető elérhető az alábbi linken: https://www.dailymail.co.uk/news/article-7763591/AI-judges-verdicts-chat-app-brave-new-world-Chinas-digital-courts.html.

[22] Erre alkalmazzák a *COMPAS (Correctional Offender Management Profiling for Alternative Sanctions)* szoftvert, amely a rendelkezésre álló adatokból „kiszámítja", a bűnelkövetők bűnismétlési esélyét korábbi vagy függőben lévő vádhatósági eljárás, büntetett előélet, a szabadlábra bocsátások, lakóhely bűnügyi fertőzöttsége, foglalkozás, szociális viszonyok és káros szenvedélyek alapján. Ezek figyelembevételével egy 1–10-ig terjedő skálán értékeli az elkövető visszaesésének esélyét, amelyre később a bíróság a szabadlábra bocsátásról szóló döntését alapíthatja, lényegében az adminisztratív előkészítő feladatokat teljes körűen elvégezve.

5. A MESTERSÉGES INTELLIGENCIA A TÁRSADALOM HIBRID FENYEGETÉSEK, ROSSZINDULATÚ INFORMATIKAI TEVÉKENYSÉGEK ÉS DEZINFORMÁCIÓ ELLENI VÉDELMÉBEN

A mesterséges intelligencia (ideértve a virtuális asszisztenseket, specifikus képelemző és kereső szoftvereket, hang- és arc[kép]felismerő rendszereket, valamint a robotokat, önvezető autókat és drónokat), valamint a dezinformációs műveletek, az álhírekkel történő operáció a lakosság tömeges és súlyos megbetegedésének kockázatát hordozó járványos betegség magyarországi megjelenése és gyors terjedésekor, egymás hatását erősítő, egy adott országgal szembeni (nemzetbiztonsági) kombinációként (műveleti intézkedések sorozataként) is felfogható. A hatályos NBS által azonosított biztonsági kockázatokkal szembeni hatékony fellépés rögzítése iránti kormányzati igény esetén cél lehet a szélesebb összhang megteremtése a teljes biztonsági szektor vonatkozásában. Az NBS által rögzített, súlyos megbetegedés kockázatát hordozó járványos betegség magyarországi megjelenése esetében is használható a mesterséges intelligencia, például a repülőtereken végzett hőképalkotáshoz, valamint a betegség terjedésének nyomon követésére szolgáló adatok gyűjtéséhez is, utóbbi esetekben a „védelmet" erősíti, tényeken alapuló információkkal az esetleges álhírek (pánikkeltés, befolyásolás) ellen. Bizonyos mesterséges intelligenciát használó alkalmazások képesek felderíteni az álhíreket és a dezinformációt a közösségi médiából származó adatok vizsgálatával, az ún. klikkvadász címeket vagy ijesztő szavakat keresve, és igyekeznek meghatározni, mely internetes forrásokat tekinthetünk hitelesnek. A publikáció készítésekor is zajló orosz–ukrán konfliktus vonatkozásában is rendkívül fontos, hogy a jelentős mennyiségű álhír között hiteles tájékoztatást lehetővé tevő információforráshoz jusson a közvélemény is, hiszen mindkét fél elemi érdeke a tisztánlátás és a hamis, illetve hamisított hírek által gerjesztett provokáció okozta hisztéria elkerülése. A háború eszkalálódása a nemzetközi közösség tudatának befolyásolása nélkül nehezen képzelhető el, abban az esetben, ha a felek a hadviselés jelenlegi földrajzi keretei között maradnak. A befolyásolás elleni küzdelem egyik leghatékonyabb eszköze pedig az idegen, illetve ellenérdekelt információs műveletek elleni hatékony, közös fellépés a NATO-n és az EU-n belül. A küzdelemben pedig a mesterséges intelligencia a folyamatos adatfeldolgozás, a minták felismerése és a támadások visszakövetése során a kibertámadások és más kiberfenyegetések kivédésében jelentős funkciót láthat el.

A fenti fenyegetettségekre reagáló dokumentumok közül kiemelve az egyik legveszélyesebb kihívás elleni védekezést szolgáló intézkedési koncepciót,[23] az Európai Unió 2019–2024 közötti időszakra vonatkozó stratégiai menetrendje a társadalom

[23] A reziliencia és a hibrid fenyegetések kezelésére szolgáló képességek megerősítése, Európai Bizottság, 2018 (https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52018JC0016&from=GA).

hibrid fenyegetések, rosszindulatú informatikai tevékenységek és dezinformáció elleni védelmének fontosságát jeleníti meg[24], valamint hangsúlyozza, hogy az ilyen veszélyek kezelése átfogó vizsgálatot igényel, több együttműködéssel, koordinációval, erőforrással és jelentős technológiai eszközpark bevetésével. Fontos megjegyezni, hogy a mesterséges intelligencia napjaink digitális forradalmának központi eleme, és az EU egyik fő prioritása. Ez a „jogalkotási célterület" azért meglehetősen bonyolult, mert a tevékenység leginkább a nemzetállamok elszigetelése, hiteltelenítése útján valósul meg, vagyis – akár az EU, akár a NATO esetében – a tagállamok egymás iránti bizalmának csökkentése a cél. Ennek ellensúlyozására válik elengedhetetlenül fontossá az ellenséges hírszerzési tevékenységgel szembeni ellenálló képesség erősítése. A tagállamok egymás közötti, illetve a tagállamok és más érintett nemzetközi szervezetek közötti szoros együttműködés, különösen a NATO-val, támogatná az EU-ban végzett ellenséges tevékenységekkel szembeni kémelhárítás összehangolását.[25] Ehhez társul továbbá, hogy a hibrid hadviselés, mint nem katonai, vagyis a nem hagyományos stratégiai kihívásokkal szemben adható válaszok (tényleges intézkedések), illetve az ezt követő, valószínűsíthető katonai tevékenység jelentős költségvonzattal jár. A nemzetközi szerepvállalás alanyaként, Magyarország vonatkozásában nem szabad elfeledni, hogy *„kiemelt jelentősége van annak a szempontnak, hogy a »korlátozott erőforrásokkal« rendelkező államok esetében a nemzetbiztonsági struktúrák hatékony működtetése, a koordinációs, irányítási, a technikai és az emberi erőforrásokra épülő információgyűjtő, az elemző-értékelő, vagy akár a különböző szakértői területek összehangolt munkája"*[26] ténylegesen összeadódjon, és így kerüljön felhasználásra akár a fenyegetések felderítése és elhárítása, akár Magyarország nemzetbiztonsági érdekeinek, céljainak érvényesítésekor.

Jogi normaalkotási aspektusból jelentős szerepet képviselnek az Európai Tanács mellett működő horizontális hibrid fenyegetések és a dezinformációs munkacsoport is. Mivel ez a szervezet közvetlenül az Állandó Képviselők Bizottsága alárendeltségében működik, képes lehet a hibrid fenyegetések elleni EU-szintű kezdeményezés, illetve tevékenység koordinálására. Fontos szerepe lehet továbbá az uniós szintű erőfeszítések támogatásakor az EU támogatásával Helsinkiben létrejött Hibrid Fenyegetések Elleni Kiválósági Központnak, amelyhez Magyarország 2019. december 10-én csatlakozott. A Központ jelentőségét növeli, hogy a NATO támogatását is magáénak mondhatja, elég csak a PACE17 kibergyakorlat körülményeire utalni. Az

[24] Az Európai Parlamentnek és a Tanácsnak A hibrid fenyegetésekkel szembeni fellépés közös keretéről szóló közös közleménye (https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52016JC0018).

[25] A reziliencia és a hibrid fenyegetések kezelésére szolgáló képességek megerősítése, Európai Bizottság, 2018. (https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52018JC0016&from=GA).

[26] Dobák Imre: Nemzetbiztonsági szolgálatok - Betekintés a visegrádi országok (V4) nemzetbiztonsági rendszereibe. *Hadtudomány,* 2015/4. szám, 114. o.

ilyen szintű joginorma-előkészítő, illetve -kibocsátó szervezetek képesek arra, hogy akár a kiberhadviselés, akár a járványkezelés, akár a hibrid hadviselés témakörében közösségi szintű, igazán hatékony stratégiá(kat) alkosson. Kellően autentikus kibocsátó szervezet erre irányuló jogi aktusa hiányában a nemzetközi együttműködés – jogi háttere – nem biztosított, azonban ennek kiadására irányuló folyamatok zajlanak az Európai Parlament szakbizottságai előtt.

A biztonsági szektor korábban megjelenített korlátokkal keresztülszabdalt jogterületét vizsgálva megállapíthatjuk, hogy az alapjogok érvényesülésének vizsgálatát eszközül használva elvégezhető az úgynevezett jogi sérülékenységvizsgálat. Ez a tevékenység a különleges jogrend idején hozott jogszabályok tekintetében széles körben megjelent a sajtóban, egyes civil szervezetek minden érintett jogszabályt ellenőriztek, és feltárták azok hiányosságait. A jogi sérülékenységvizsgálat az előkészítése a célzott támadásnak, a lawfare eszközrendszere alkalmazásának. A stratégiaalkotók és a kibocsátók szempontjából is célszerű erre a körülményre is figyelemmel lenni, mivel a hibrid hadviselés láthatatlan fegyvere a lawfare. Az ilyen jellemzőkkel körülírható (relatíve új típusú) fenyegetettség jelenléte a nemzetközi színtéren egyre alaposabb és időtartamát tekintve egyre kiterjedtebb.

A hadviselő fél az összehangolt tevékenységsorozat közben a modern technológiák és eszközrendszerek által nyújtott képességeket, opciókat használja fel, és műveleteit kiterjeszti a kibertérre, a média világára, a gazdaságra és a társadalmi érintkezés különböző formáira is. Az egyes elemek (támadási formák) önálló vagy egymást kiegészítő (kombinatív) alkalmazása – a klasszikus támadási formák bevetése nélkül is – már alkalmas lehet a befolyásolásra, a zavarkeltésre, egyes államok belső rendjének a megbontására, társadalmi tudat újraformálására. Az új típusú fenyegetettség fokozott szintjére tekintettel Magyarország kiemelt feladatként tekint a hibrid fenyegetések elleni fellépésre, illetve azok kezelésére. Ez a hatályos NBS-ben is rögzítésre kerül, ugyanakkor a lawfare kapcsán még csak a kifejezés jelentésével és a potenciális veszélyforrás alapvető tulajdonságaival ismerkedik a jogalkotó és a legtöbb szakmai szervezet.

***

A mesterséges intelligencia alkalmazásának számos területe közül az adatanalitika és a döntés-előkészítés, esetleges döntéshozatal vonatkozásában fontos megjegyeznünk,[27] hogy *„a technológiai fejlődés a joggal szemben ambivalens követelményeket támaszt: egyrészről a jog szabályainak újragondolását indukálja annak érdekében, hogy a technológiai fejlődés ne ássa alá az emberi szabadságjogokat. Ugyanakkor*

[27] Klein Tamás – Tőth András: A robotika egyes szabályozási kérdései. In Homicskó Árpád Olivér (szerk.): *Egyes modern technológiák etikai, jogi és szabályozási kihívásai.* Budapest, Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, 2018, 94. o.

azt is biztosítani kell, hogy a jog ne akadályozza a technológiai fejlődést." Ez a kettősség határozza meg szűkebb értelemben vett jogalkalmazói és a jogalkotói döntéseket támogató nemzetbiztonsági funkciókat is. Elég a külső engedélyhez kötött titkos információgyűjtés egyik engedélyezési eljárására gondolnunk, és máris a humán bírósági és magyarországi, választott országgyűlési képviselők biztosította politikai kontroll fontosságát kell megvizsgálnunk. Lehetséges-e a titkosszolgálatok működése feletti ellenőrzés legfontosabb eszközeit automatizálni, ráadásul olyan virtuálisan létező adatok alapján, melyeket a mesterséges intelligencia vélhetően nem is ismer teljes mértékben? Minden állam alapvető érdeke, hogy ne digitalizálja minden adatát, hiszen ha az adat érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele közvetlenül és tartósan sérti vagy veszélyezteti Magyarország szuverenitását, területi integritását, törvényes rendjét, belső stabilitását, vagy visszafordíthatatlanul jelentős károkat okoz az ország honvédelmi, nemzetbiztonsági, bűnüldözési, igazságszolgáltatási, központi pénzügyi és gazdasági érdekeiben, külügyi és nemzetközi kapcsolataiban, a szövetséges tagállamokkal közös biztonsági érdekeiben, akkor ezeknek a védelme érdekében indokolt lehet az, hogy ne legyenek „betáplálva" egy döntés-előkészítő rendszerbe. Az előbbiek általi ellenőrzést és a szolgálatok tevékenységének titkossága közötti egyensúlyt célszerű fejleszteni, úgy, hogy a minősített adatok megismerésére jogosultak köre, az eljárás nyilvánossága a szükséges mértékben korlátozható maradjon. Minden egyes eset jogszerűségének vizsgálatára kiterjedő, külső szerv hatáskörébe tartozó, hatékonynak minősíthető eljárás keretében végezhető ellenőrzésről szóló törvényi szabályozás nélkül a magánéletbe való állami beavatkozás aránytalan korlátozásnak minősülhet, megítélésem szerint a humán kontroll nélküli döntések ebbe a körbe tartoznának, így ez jelenti a mesterséges intelligencia alkalmazhatóságának határát. Enélkül ugyanis nincsen biztosítva annak a mérlegelésnek a független felülvizsgálása, amely a magánélet titkos eszközökkel való kifürkészésének szükségességéről, arányosságáról és célhoz kötöttségéről szól. A bíróságra tartozó kérdés az, hogy a titkos információgyűjtés tervezett alkalmazásával elhárítani kívánt veszély és a magánélete rejtett megfigyelését elszenvedni kényszerülő személynek okozott hátrány a konkrét esetekben arányban áll-e. Ugyanakkor a politikai, illetve diplomáciai súllyal bíró ügyek esetében az engedélyezést továbbra is a választópolgárok által megválasztott Országgyűlés által támogatott Kormány felelősségi körében volna indokolt tartani. Nyilván az információ és adatkezelési redundancia hiánya, illetve az adatfúzió okozta központosítás okozhatja még a teljes kompromittálódást is a védendő adatok vonatkozásában. A megalapozott döntésekhez pedig a rendelkezésre álló összes adat ismerete és szakértői felhasználása szükséges, amely nagyon komoly előrelátást is igényel a gépi tanulás útján is megszerezhető tapasztalat és lexikális tudás mellett.

Utóbbiak birtokában jelentős előnyre tehet szert a rendvédelmi, illetve nemzetbiztonsági ágazat, különösen egy információfúziót végző szerv, azonban a felhatalmazással járó kiemelt felelősség kérdésének vizsgálata során nem szabad elfeledni Lukács evangélista[28] által figyelmünkbe ajánlottakat: *Mind kinek sokat adtak, sokat kérnek tőle; és akire sokat bíztak, attól többet kívánnak.*

[28] Lukács Könyve 12:48.

GÁL ISTVÁN – BARTKÓ RÓBERT

A kibertérben megjelenő kihívások és fenyegetések büntetőjogi kezelésének tendenciái

A kibertérben megjelenő kihívások és fenyegetések büntetőjogi kezelésének tendenciái témakörön belül elsősorban a terrorizmussal, illetve a terrorizmus finanszírozásával foglalkozunk e tanulmány keretein belül; valamennyi kihívás és fenyegetés büntetőjogi vonatkozásainak bemutatására egy kismonográfia terjedelmi keretei sem lennének elegendők. Mindezt erősíti a kibertér jelentette kihívások összetett halmaza, amelynek politikai-társadalmi, illetve komplex biztonsági vonatkozásai is megjelennek jelen kötetben.

A terrorizmusnak mind a hagyományos, mind az online térben terjedő formái számos biztonságpolitikai kérdést vetnek fel, egyúttal azonban a büntetőjog számára is generálnak szinte feloldhatatlannak tűnő dilemmákat, melyek a kérdéskör tágabb jogi és államszervezési kérdéseitől sem függetlenek. Ezek közül egyet megemlítve, a terrorizmus egyik legveszélyesebb fajtája, az öngyilkos merénylet a hagyományos büntetőjogot megoldhatatlan probléma elé állítja napjainkban. A büntetőjognak ugyanis az egyik kiindulópontja az, hogy a kilátásba helyezett szankciónak van – több vagy kevesebb – visszatartó hatása. A visszatartó hatás egészen pontosan két tényezőtől függ egy adott bűncselekmény elkövetője tekintetében: a kilátásba helyezett szankció súlyosságától és az adott bűncselekmény felderítési mutatójától. (Rögtön hozzá is tehetnénk, hogy Beccaria szerint a második tényező a hangsúlyosabb, azaz a visszatartó hatás nem a büntetés súlyosságától, hanem annak elmaradhatatlanságától várható, de ez a kérdés a vizsgált téma szempontjából nem sok relevanciával bír.)

A nagy probléma az, hogy az öngyilkos merénylőt miként tartsuk vissza? Még ha a legsúlyosabb büntetést helyeznénk is kilátásba, lenne-e visszatartó ereje annak, ha kijelentjük: az elfogott öngyilkos merénylők halálbüntetésre számíthatnak? Van-e visszatartó ereje annak, ha az öngyilkos merénylő ezzel számolhat? Vagy ha esetleg azt is be kell kalkulálnia, hogy az akció végrehajtása közben lelövik? Véleményem szerint egyáltalán nincs! *Az öngyilkos merénylőt a büntetőjog jelenlegi eszköztárával nem lehet visszatartani, egyszerűen azért, mert neki nincs veszítenivalója.* A legtöbb, amit veszíthet, hogy nem a tervezett helyen és időben, hanem pár kilométerrel arrébb és kicsit korábban vagy később hal meg.

A büntetőjog tehát egyszerűen csődöt mond az egyik legsúlyosabb modern bűnözési formával szemben! Ezzel a szituációval bizonyos értelemben analógiát mutat

a kibertérben elkövetett terrorizmus és a terrorizmus finanszírozása elleni büntetőjogi és büntetőjogon kívüli jogszabályok hatékonyságának a problémaköre.

A múlt század végén a terrorizmus alapvető motivációja az anarchizmus és a nacionalizmus volt – s noha a jelenkor terrorizmusa számára ez csak történelem, eszmeviláguk több alkotóeleme is felbukkan a későbbi korszak terrorcselekményeinek indoklásában, illetve szolgált motivációként. Más volt az eszközrendszerük is – tőr, méreg, pokolgép –, a századfordulón merényletek sorozatát követték el, államfők és uralkodók ellen, kezdve a sort Carnot francia elnökkel, folytatva egészen Erzsébet királynéig.[1]

Ettől függetlenül kijelenthetjük, hogy maga a terrorizmus jellegzetesen 20. századi jelenség, és komolyabb problémaként először csak a második világháborút követő időszakban jelentkezett, főként három földrajzi térségben: Nyugat-Európában, Közel-Keleten és Latin-Amerikában.

„A terrorizmus eltérő eszmerendszerekből merítő, sajátos logikának engedelmeskedő, változatos formákat öltő módszeres erőszak-alkalmazás, vagy ezzel való fenyegetés, melynek célja politikai törekvések elérése azáltal, hogy az áldozatban, a nézőközönségben, az államban, a társadalomban megalkuvó magatartás alakuljon ki. A meghirdetett cél általában politikai, ideológiai, vallási, etnikai stb. tartalmú radikális változás kikényszerítése, a cél elérésére alkalmazott cselekménysor. Az eszköz viszont jogi lényegét tekintve köztörvényes, erőszakos bűncselekmény."[2]

A jövő legfontosabb kihívásai a nukleáris terrorizmus, az ökoterrorizmus, a biológiai terrorizmus, a kibertérben elkövetett terrorizmus, és egyre komolyabb problémaként kell számolni a vallási alapon szerveződött radikális terrorcsoportok tevékenységével.

A terrorizmussal foglalkozó tanulmányok megegyeznek abban, hogy a terrorizmus alapvetően politikai jelenség, amely mögött strukturális és pszichológiai tényezők egyaránt vannak. Általános vélekedés, hogy a modernizáció, a demokrácia és a kezeletlen szociális feszültségek teremthetnek olyan feltételeket, amelyek életre hívják a terrorizmust.

A terrorcselekmények veszélyessége a váratlanságban, a kiszámíthatatlanságban és a gyors, mobil csapásmérő képességben rejlik. A régi korok klasszikus és a jelenkor terrorizmusa között elsősorban minőségi a változás, de a legfontosabb különbségek mégis a történelmi fejlődésből alakultak ki.[3]

Ahogy a terrorizmus mai modern formájának sincsenek évszázados gyökerei, még erőltetettebb a terrorizmus elleni küzdelem jogtörténetéről beszélni. Ennek

[1] Szövényi György: A terrorizmus jellegzetességei az ezredfordulón. *Európai Tükör*, 1998/3. szám, 92. o.

[2] Korinek László: A terrorizmus. In Gönczöl Katalin – Kerezsi Klára – Korinek László – Lévay Miklós (szerk.): *Kriminológia-Szakkriminológia.* Budapest, CompLex Kiadó, 2006, 447. o.

[3] Gergely Attila: A terrorizmus természetrajza. *Kapu*, 1994/10–11. szám, 92. o.

előrebocsátása után idézünk egy száztíz éves jogesetet, amelyet a saját korában állam elleni bűncselekménynek minősítettek, de talán a terrorizmus finanszírozása kriminológiai értelemben vett fogalma egyik korai megnyilvánulási formájának is tekinthetjük:

„M. I. félrevezettetvén a szoczialisták izgatásaitól, és a megtévesztett munkás-elemek általános elégületlenségétől, és félreismerve az állami és társadalmi rend fenntartó s éltető intézményeit, arra a gondolatra jutott, hogy a munkásosztálybeliek helyzete a jobb sorsban levőkkel szemben visszás, a minek a jelenlegi állami rend az oka: ezt megváltoztatni, vagy megbosszulhatni vélte azzal, ha a koronás király élete ellen merényletet tervez és merényletét sikerrel követi el. Elhatározta tehát, hogy a királyt megöli. Miután azonban e tervhez társra volt szüksége, ilyent keresett és talált is a hozzá hasonló H. L. személyében. M. I. és H. L. együtt megbeszélték a tervet, hogy a királyt dinamitrobbantással kellene elpusztítani, amire alkalmas a Margit-körúti csatornavonal, melyet mindketten ismertek. A dinamitot keresetükből kívánták beszerezni. Mivel azonban annyi keresetük nem volt, hogy e czélra megfelelő összeget fordíthattak volna, M. I. egy olyan embert keresett, a ki a szükséges pénzt vagy a robbantó szert megszerezheti. K. Gy.-t mindketten a közvágóhídnál folyt csatornamunkálatok idejéből ismerték: tudták, hogy ez híve V. I.-nek, kinek izgatásairól hallottak; azt is tudták, hogy V. I. gazdag ember, és gondolták, hogy bűnös czéljukra K. Gy útján a szükséges anyagi eszközöket megszerezhetik. Közölték tehát a tervet K. Gy-val, aki azt helyeselte és 500 frtnak szerzését helyezte kilátásba. Így szövetkeztek M. I., H. L. és K. Gy. mindhárman együtt 1898. évnek elején arra, hogy Ő Felségét, a királyt életétől megfosszák. A tervet mindhárman megbeszélték, annak dinamitrobbantás útján történő keresztülvitelét tárgyalták egy oly vonalon, amelyen a király Budapesten időzése alkalmával elhaladni fog. A terv azonban a részletes megvalósítás stádiumába nem került: vádlottak előkészületeket nem tettek, pusztán szövetségre léptek egymással a király élete elleni merénylet czéljából."[4]

A 19. század végén Sztálin és társai oroszországi akcióikhoz bankrablásokból teremtették elő a szükséges pénzt, a 20. század második felében a Baader–Meinhof-csoport[5] tagjai is hasonló módszerekkel jutottak anyagi eszközökhöz. Mára ez a fajta finanszírozás kivételnek számít, ahogy erre Korinek László is rámutat.[6] Napjaink terroristái szívesebben nyúlnak a szervezett bűnözés kipróbált megoldásaihoz, valamint a kibertérben is keresnek finanszírozási forrásokat.

[4] Edvi Illés Károly: *Az anyagi büntető törvények és a sajtótörvény.* Budapest, Grill Károly Könyvkiadó Vállalata, 1907, 217. o.

[5] Lásd részletesen Gerhard Wisnewski – Wolfgang Landgraeber – Ekkehard Sieker: *Das RAF-Phantom Neue Ermittlungen in Sachen Terror.* München, Knaur Taschenbuch Verlag, 2008, 512. o.

[6] Korinek: i. m. (2006), 455. o.

1. TERRORIZMUS A KIBERTÉRBEN

Az elmúlt század 60-as éveitől kezdődő modernizációs és globalizációs törekvések egy egységes térré törekedtek formálni az addig bipoláris módon felépített világrendünket. Az említett folyamatok a terrorizmus történetében is meghatározó jelentőségűek, hiszen azok kölcsönhatásában[7] a terrorizmus úgy vált posztmodern korunk szerves részévé, hogy idomulva ahhoz, az transznacionálissá és sok esetben virtuálissá is vált.[8] Ezáltal pedig kihasználhatta az indusztriális és információs társadalomban rejlő lehetőségeket. Ebben a formálódásban, „fejlődésben" jelentős szerepet játszott az informatika fejlődése, a technológia új vívmányainak megjelenése, az internet világméretűvé válása is, mely a terrorista hadviselés számára egyértelműen új távlatokat nyitott. Az ún. konvencionális terrorizmus mellett „a paletta színesedett" a tömegpusztító fegyvereket alkalmazó, valamint a számítógépes terrorizmussal is[9] (összefoglaló nevén: „ABC-terrorizmus"), utóbbi pedig a kibertérben rejlő lehetőségeket is kiaknázta.

Az információ áramlásának új, az internetnek is köszönhetően felgyorsult módja egyrészt gyökeresen alakította át, és vélhetően a jövőben tovább is fogja formálni a biztonságpolitikai kihívásokat és az azokra adott válaszokat,[10] ideértve természetesen a jogi természetű válaszokat is,[11] másrészt erősítette a nemzetközi terrorizmus egyik fő ismertetőjegyét, a láthatatlanságot[12] is.

A terrorizmus a maga „régi, hagyományos formájában" közvetlenül a minket körülvevő társadalom feszültségeire reagált, a kriminalitás ezen természete pedig nem változott semmit a technológiai fejlődéssel sem. A technológia, amely – Kelemen Roland álláspontját osztva – alapvetően egy olyan szociális konstrukció, mely révén a hagyományos tér folyamatai összefonódnak a kibertér folyamataival, fejlődésének eredményeként a hagyományos társadalmi konfliktusok a kibertér belső rendszerében is megjelentek,[13] lehetőséget és teret adott és ad mind a mai napig a büntetőjog terrénumához tartozó extremitásoknak, azok térnyerésének.

[7] A terrorizmus és a globalizáció kapcsolatára vonatkozóan lásd bővebben Bartkó Róbert: *A terrorizmus elleni küzdelem kriminálpolitikai kérdései.* Győr, UNIVERSITAS-Győr Nonprofit Kft, 2011, 70–79. o.

[8] Rostoványi Zsolt: Terrorizmus és szabadság. *Fundamentum,* 2001/4. szám, 56. o.

[9] Lásd erről a kérdésről bővebben Korinek László: *Kriminológia.* Budapest, Magyar Közlöny Lap- és Könyvkiadó Kft., 2010, 413. o.

[10] A 21. századi biztonsági kihívásokról lásd bővebben Farkas Ádám: Gondolatok a 21. századi biztonságról, államról, védelemről. *Hadtudomány,* 2018/elektronikus szám, 241–256. o.

[11] A modern technológiai vívmányok jogi kihívásai tekintetében lásd Nagy Zoltán András: A jövő tegnap óta tart. A modern technikai-technológiai folyamatok kihívásai a jog területén. *Belügyi Szemle,* 2018/10. szám, 36–55. o.

[12] A modern kori terrorizmus főbb ismérvei tekintetében lásd Bartkó: i. m. (2011), 67. o.

[13] Kelemen Roland: A kibertérből érkező fenyegetések jelentősége a hibrid konfliktusokban és azok várható fejlődése. *Honvédségi Szemle,* 2020/4. szám, 70. o.

Más kriminalitáshoz hasonlóan a technológia innovációi, az internet, az okos eszközök, az információs hálózatok használatának fejlődése,[14] a digitális kommunikáció egyre változatosabb csatornái[15] a terrorizmus tekintetében is új elkövetési módokat alakítottak ki, és bővült azoknak a cselekményeknek a köre, mellyel szemben az anyagi büntetőjognak is szükséges fellépnie.

Elfogadva a szakirodalmi álláspontot, a terrorizmus megjelenése a kibertérben alapvetően két síkon értelmezhető. Egyrészt a tulajdonképpeni, szűkebb értelemben vett kiberterrorizmus vagy számítógépes terrorizmus síkján, másrészt a terroristák, terrorista szervezetek egyéb internetes tevékenysége[16] vonatkozásában.[17] Előbbi a kibertérben, annak felhasználásával elkövetett terrorista akciókra utal, míg utóbbi olyan célokra fókuszál, melyek részben konkrét törvényi tényállások szintjén is értékelt a jogalkotók által, részben pedig olyan „büntetlen cselekmények", melyek akár a szervezet létezéséhez, működéséhez, akár későbbi akciók végrehajtásához kapcsolódhatnak. Alisdar A. Gillespie nyomán Dornfeld László ezeket a célokat az alábbiakban foglalja össze:[18] a terrorista propaganda térnyerésének biztosítása; a pénzgyűjtés; az információterjesztés, valamint a biztonságos kommunikáció és hírszerzés.[19]

A nemzetközi terrorizmus ezen megváltozott, összetett jellege nemcsak a katonai, biztonságpolitikai, de a (büntető) jogi válaszok terén is újabb kihívást jelentett a demokratikus jogállamok számára, az egységes fellépés szándéka azonban az utóbbi évtized jogalkotási fejlődésében – főként az Európai Unió szintjén – egyértelműen tetten

[14] Mezei Kitti: A modern technológiák kihívásai a büntetőjogban, különös tekintettel a kiberbűnözésre. *Állam- és Jogtudomány*, 2020/4. szám, 66. o.

[15] Mezei Kitti – Szentgáli-Tóth Boldizsár: Az online platformok használatában rejlő veszélyek: a dezinformáció és a kibertámadások jogi kockázatai. In Chronowski Nóra – Szentgáli-Tóth Boldizsár – Szilágyi Emese (szerk.): *Demokrácia – Dilemmák. Alkotmányjogi elemzések a demokráciaelv értelmezéséről az Európai Unióban és Magyarországon.* Budapest, ELTE Eötvös Kiadó, 2022, 241. o.; Kelemen Roland: Radikalizálás, dezinformálás és tömegpszichózis modern köntösben: a hibrid konfliktus kibertérben. *Jog Állam Politika,* 2021/3. szám, 75–77. o.

[16] Neparáczki Anna Viktória az előbbit az információtechnológia „hard" típusú, míg a másodikat az ún. „soft" típusú felhasználásaként jelöli meg munkájában. Lásd ezzel kapcsolatban: Neparáczki Anna Viktória: A kiberterrorizmus büntető anyagi jogi megítélése. *Ügyészek Lapja,* 2020/1. szám, 71–85. o.

[17] Dornfeld László: Kiberterrorizmus – a jövő terrorizmusa? In Mezei Kitti (szerk.): *A bűnügyi tudományok és az informatika.* Pécs, Budapest, PTE ÁJK – MTA Társadalomtudományi Kutatóközpont, 2019, 53. o.

[18] Dornfeld: i. m. (2019), 53. o.

[19] Ha megvizsgáljuk az egyes célokat, könnyen belátható a tézis igazolt volta. A propaganda rendkívül fontos a terroristák és a terrorszervezetek szempontjából, hiszen személyi bázisuk fejlesztésére és a megfélemlítési célzat hatékonyabb közvetítésére is alkalmas. Ugyanez mondható el a pénz- és információgyűjtési célzatról is, melyek szintén fontos a terrorszervezetek és -csoportok létrehozása, működtetése, az egyes akciók előkészítése szempontjából. A biztonságos kommunikáció és a hírszerzés pedig annak záloga, hogy ezen szervezetek a hatóságok előtt észrevétlenek tudjanak maradni, akár konspiratív jellegüket is erősíthetik.

érhető. A kibertérben megvalósuló terrorista aktivitásokkal szembeni fellépés szükségességét a közelmúlt migrációs eseményei és az annak nyomán megvalósult terrorista akciók, a támadások legitim voltát igazoló elvek, azaz a propaganda szélesebb körben történő terjesztése is indokolták. Ezek a folyamatok rámutattak arra az európai integráción belül is, hogy a nagyrészt liberálisnak tekinthető migrációs politika komoly biztonsági deficitet okozhat.[20] Az említett migrációs nyomás okozta megingott biztonsági környezet a kibertér, az internet adta lehetőségek mellett az egyes terrorszervezetek számára komoly hálózatépítési, hálózatfejlesztési lehetőségeket teremtett.[21]

A tanulmány jelen szerkezeti egységének ezért az a célja, hogy bemutassa, a hazai büntetőjog – figyelemmel az Európai Unió által is támasztott elvárásokra – miként próbál fellépni a kibertérben megjelenő terrorizmussal szemben. Azaz célunk nem a fogalomalkotás, hiszen ennek a kérdésnek hazánkban alapvetően kiforrott szakirodalma van.[22] Elemzésünk során inkább a kiberterrorizmushoz kapcsolódó jelenségek büntető anyagi jogi vetületeire koncentrálunk majd, illetve kitérünk azokra a területekre, magatartásokra is, melyek „szürke foltként" értékelhetők a kriminalizáció folyamatában. Nem célunk ugyanakkor a kiberbűnözéssel általános, elméleti szinten foglalkozni, hiszen az, annak számtalan területe révén, szétfeszítené a tanulmány e részének célját és kereteit, ezért kifejezetten csak anyagi büntetőjogi kérdésekre fókuszálunk. Az elemzés során külön értékeljük hazánk anyagi jogi fellépését a tulajdonképpeni kiberterrorista cselekmények, valamint a terroristák egyéb internethasználati cselekményei esetében.

2. A KIBERTERRORIZMUS KRIMINALIZÁLÁSA A HAZAI BÜNTETŐJOGBAN

Az Európai Parlament 2017. február 16. napján fogadta el a terrorizmus elleni uniós szintű küzdelem módosított jogi kereteit megfogalmazó 2017/541 számú Irányelvet (a továbbiakban: Irányelv), mely jelenleg az Európai Unió valamennyi tagállama

[20] Böröcz Miklós: Az Európai Unió közös kül-, és biztonságpolitikájának néhány főbb kihívása napjainkban. *Terror & Elhárítás*, 2013/2. szám, 81. o.

[21] Migráció és terrorizmus kapcsolata tekintetében lásd bővebben Bartkó Róbert: *Az irreguláris migráció elleni küzdelem eszközei a hazai büntetőjogban.* Budapest, Gondolat Kiadó, 2020, 128–147. o.

[22] Lásd ebben a körben az alábbi fontosabb hazai munkákat: Neparáczki: i. m. (2020); Nagy Zoltán András: Kiberbűncselekmények, kiberháború, kiberterrorizmus – avagy ébresztő Magyarország! *Magyar Jog*, 2016/1. szám, 17–24. o.; Szádeczky Tamás: Terrorizmus a kibertérben. *Infokommunikáció és Jog*, 2008/5. szám, 200–205. o.; Mezei Kitti: *A kiberbűnözés aktuális kihívásai a büntetőjogban.* Budapest, TKJTI, L'Harmattan, 2020; Lajtár István: A kiberbűnözésről. *Ügyészek Lapja*, 2019/1. szám, 47–52. o.; Ambrus István: *Digitalizáció és büntetőjog.* Budapest, Wolters Kluwer Hungary Kft., 2021; Mezei, Kitti: Cyberterrorism – How real is the threat? In Szőke, Gergely László (szerk.): *Studia Iuridica Auctoritate Universitatis Pécs Publicata. Essays of Faculty of Law University of Pécs Yearbook of 2017–2018.* Pécs, Pécsi Tudományegyetem, 2020, 59–75. o.

számára – felváltva a korábbi kerethatározati szabályozási rendszert – a fellépés fundamentális kereteit rögzíti. Az Irányelv célja, hogy szélesítse a büntetendővé nyilvánítandó cselekmények körét, külön kiemelve annak a követelményét, hogy a tagállamoknak az interneten történő elkövetéssel szemben is biztosítaniuk kell az anyagi büntetőjogi fellépés lehetőségét.[23]

Az Európai Unió ezen jogalkotási lépése illeszkedik ahhoz a folyamathoz is, amely a terrorizmus elleni tagállami fellépésben a büntetőjogi eszközök mellett a közjogi és védelmi jellegű eszközök megerősítését is célozta.[24]

Az Európai Unió már több jogi dokumentumában, így az irányelvben is rögzítette, hogy a terrorcselekmények jelentik a legsúlyosabb támadást az Unió alapértékeinek tekinthető jogállamiság és demokrácia ellen.[25] Minthogy a terrorizmus súlyos fokban veszélyezteti az Unió által képviselt demokratikus értékeket, az Irányelv a büntetendővé nyilvánítandó magatartások körének bővítésével törekedett elérni a fellépés hatékonyságának fokozását. Ennek megfelelően a terrorcselekmény tényállása mellett külön szabályozásra kerülnek a terrorizmussal összefüggő bűncselekmények, melyek révén az Unió azt reméli, hogy a terroristagyanús személyek még egy adott akció végrehajtása előtt – az előkészítő fázisban, vagy akár még azt megelőzően – kiemelhetők lesznek a társadalomból. Az Irányelv egyebekben az Unió átfogó terrorizmusellenes politikájának fontos, jogi részét képezi, mely politikát egyebekben további más elemek – így az Europol és az Eurojust munkája, a különféle cselekvési tervek és politikai szinten megfogalmazott stratégiák, az Unió külső határainak ellenőrzésére irányuló tevékenység – is kiegészítenek.[26]

[23] Az Irányelv a Preambulum (6) bekezdésében utal arra, hogy a büntetendővé nyilvánítandó magatartások büntetni rendeltségét akkor is biztosítani kell, ha az interneten keresztül vagy a közösségi média felületek közbeiktatásával kerülnek elkövetésre, míg a (11) bekezdés a toborzás, kiképzés, a (22) bekezdés pedig a nyilvános uszítást megformáló online tartalmakkal szembeni fellépések körében támaszt ilyen követelményeket.

[24] Lásd ezzel kapcsolatban a hazai szakirodalomban: Simicskó István: A terrorizmus elleni védelem fokozása a különleges jogrendi kategóriák bővítésével. *Hadtudomány*, 2016/3–4. szám, 100–113. o.; Farkas Ádám: A terrorizmus elleni harc, mint kiemelt ágazatközi fegyveres védelmi feladat. *Szakmai Szemle*, 2017/3. szám, 5–20. o.; Farkas Ádám: Gondolatok a terrorveszélyhelyzetről. *Szakmai Szemle*, 2016/3. szám, 174–189. o.; Kelemen Roland – Németh Richárd: A kibertér fogalmának és jellemzőinek multidiszciplináris megközelítése. In Farkas Ádám (szerk.): *Védelmi alkotmányosság az új típusú biztonsági kihívások erőterében.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2018, 147–169. o.; Kelemen Roland: Pillanatképek a kivételes állapot elméleti kérdéseinek köréből. *Katonai Jogi és Hadijogi Szemle*, 2016/1–2. szám, 65–80. o.

[25] Az Európai Parlament és a Tanács 2017/541 számú Irányelve, Preambulum (2) bekezdés.

[26] Cian C. Murphy: Counter-Terrorism Law and Policy: Operationalisation and Normalisation of Exceptional Law after the 'War on Terror. Diego Acosta Arcarazo –Cian C. Murphy: *EU Security and Justice Law: After Lisbon and Stockholm*. London, Hart Publishing Ltd., 2014, 168–169. o.

2.1. A tulajdonképpeni kiberterrorizmus elleni fellépés anyagi büntetőjogi eszközei

A szakirodalom a kiberterrorizmus fogalmához kétféleképpen közelít. Az egyik álláspont szerint kifejezetten a kiberbűncselekmény terrorista célzatú elkövetése értendő ezen kategórián. Dornfeld László véleménye szerint azonban a jelenség azokkal a terrortámadásokkal azonosítható, melyek a kibertérben kerülnek elkövetésre.[27] A szerző – nézetem szerint – helyes kiindulópontot választ, hiszen ilyen értelemben a kiberterrorizmus nem azonos egy kiberbűncselekmény terrorista célzatú elkövetésével, annál jóval tágabb kategória. Egy ettől eltérő értelmezés ugyanis jelentősen szűkítené a terrorcselekmény összetett tényállási konstrukciójában részletesen szabályozott eszközcselekmények körét.[28] Azaz a tulajdonképpeni kiberterrorizmus esetén az elkövető nemcsak önmagában egy terrorista célzatú hackertámadást követhet el információs rendszer ellen – ezzel megvalósítva az információs rendszer vagy adat megsértése eszközcselekményét –, hanem azon keresztül egyben egy másik, a Btk. 314.§ (4) bekezdés i) pontjában értékelt eszközcselekmény elkövetési magatartását is meg tudja valósítani. Ezáltal pedig cselekménye egy másik eszközcselekmény elkövetési magatartásaként, maga a számítógépes rendszer pedig a bűncselekmény elkövetésének eszközeként is minősülhet. Ilyen értelemben tehát egy terrorista akció végrehajtásának kriminalizálása egységes, függetlenül attól, hogy az a kibertér felhasználásával kerül-e elkövetésre vagy sem.

Az irányadó szakirodalom is megerősíti a fenti álláspontot, amikor az internetes vagy kiberterrorizmusnak alapvetően megkülönbözteti a tömeges pusztításra, a tömeges zavarkeltésre, valamint a társadalmi rend destabilizálására irányuló formáját. Az első kategóriában tartozhatnak tipikusan a kritikus infrastruktúrák elleni – számítógépes rendszer felhasználása révén megvalósított – terrorista célzatú támadások, míg a második alapvetően a pánikkeltésre, a lakosság megfélemlítésére, az utolsó pedig a társadalmi élet működésének ellehetetlenítésére (pl. közérdekű üzemek elleni támadások) irányul.[29]

[27] Dornfeld: i. m. (2019), 47. o.

[28] Neparáczki Anna Viktória ettől eltérő álláspontot fogalmaz meg a tanulmányban már idézett 2020-ban publikált munkájában, amennyiben az ún. „hard" típusú elkövetést tisztán a kiberbűncselekmény terrorista célzatú elkövetésével azonosítja, és törvényi szabályozottságát a Btk. 314.§ (4) bekezdés i) pontja szerinti eszközcselekményben látja azzal, hogy természetesen ilyen esetben a minősítés differencia specifikája a terrorista célzat. Ugyanakkor – ahogyan arra Dornfeld László példákban is rámutat – nézetem szerint a számítógépes rendszerekkel szemben megvalósított terrorista célzatú támadás más eszközcselekményhez, például közveszélyokozáshoz, radioaktív anyaggal visszaéléshez, vagy éppen közérdekű üzem működésének megzavarásához, jármű hatalomba kerítéséhez is kapcsolódhat.

[29] Brenner, W. Susan 2006-ban „Cybercrime, Cyberterrorism, Cyberwarfare" című, a *Revue Internationale de Droit Pénal* 3. számában megjelent tanulmányára e helyütt Dornfeld László hivatkozik már említett tanulmányának 55–57. oldalain.

Amennyiben tehát a fentiekben hangsúlyozott jogi érvek mentén elfogadjuk, hogy a terrorcselekmény tényállását egységesen kell megítélni, és nem lehet tényállástani szempontból különbséget tenni aközött, hogy a kibertér felhasználásával kerül-e sor az elkövetésre, kijelenthető, hogy a magyar Btk. összhangban van az uniós Irányelvben foglalt elvi keretekkel. A terrorcselekmény Btk.-ban szabályozott esetkörei, az egyes cél- és eszközcselekmények, valamint a tényállásokhoz kapcsolt szankciókeret is megfelel az uniós elvárásoknak, követelményeknek, azokkal kapcsolatban alapvetően módosítási igény vagy szükség nem merül fel, mely egyebekben uralkodó álláspont a hazai szakirodalomban is.

2.2. A terrorista célzatú információs rendszerhasználat egyéb vetületei

Követve a korábbiakban, a szakirodalom alapján hivatkozott felsorolást, a téma kapcsán elsődlegesen *az ún. propagandatevékenység* anyagi büntetőjogi értékelésével szükséges foglalkoznunk. Ez alapvetően kapcsolódhat általában a terrorizmusnak legitimációt adó eszmék, indokok szélesebb körben történő sugárzásához, akár egy-egy konkrét, már megvalósított akció indokainak utólagos igazolásához, de természetesen az egyének gondolkodásának befolyásolásához is, melynek eredményeként ezen személyek utóbb vagy csatlakozhatnak egy terrorszervezethez, terroristacsoporthoz, vagy „saját elhatározásból", formális hűségesküt téve „a magasztosnak hitt céloknak" maguk követnek el eseti akciókat. A fenti esetkörök vizsgálata alapján teljesen nyilvánvaló, hogy büntetőjogi fellépés azon magatartásokkal szemben indokolt, melyek közvetve vagy akár közvetlenül is hozzá tudnak járulni ezen extremitás eszkalálásához.[30]

Az Irányelv – figyelemmel az elmúlt időszak terrorista akcióira és az egyes szervezetek azzal kapcsolatosan kifejtett „propagandakampányára" – rögzíti, hogy a tagállamoknak minden olyan magatartást is büntetniük kell, amely terrorcselekmény elkövetésére irányuló nyílt felhívás céljából nagy nyilvánosság előtt közvetve vagy közvetlenül magasztalja, illetve szorgalmazza a terrorcselekmények megvalósítását.[31] Azaz ebben az esetben az elkövető a cselekmény kifejtésekor nem

[30] Az azonban fontos, hogy itt olyan propagandatevékenységről van szó, amely nem egy már konkrét és körvonalazható terrorista akció végrehajtására keres elkövetőket, szólít fel embereket, hiszen amennyiben ez a magatartás már egy konkrét terrorcselekmény elkövetési szándéka által vezérelt, akkor a klasszikus értelemben vett terrorcselekmény sui generis jelleggel szabályozott valamely előkészületi magatartásért felel az elkövető.

[31] Természetesen az Irányelv 5. cikke helyesen mutat rá, hogy csak azon szándékos magatartások lehetnek relevánsak e körben, melyek közvetve vagy közvetlenül szorgalmazzák terrorista cselekmények elkövetését, vagy annak veszélyét hordozzák magukban, hogy ilyen akciók kerülhetnek elkövetésre. Az ezen következmény kiváltására objektíve alkalmatlan propaganda kívül marad a büntető anyagi jogi fellépés terrénumán.

egy konkrét terrorcselekményhez kapcsolódik büntetendő magatartásával,[32] hanem azt mint eszközt „reklámozza" a nyilvánosság felé, azaz az uszító magatartás hatására fennáll a terrorista bűncselekmény elkövetésének, a terrorista szándék kialakulásának veszélye.

A hazai jogalkotás ezzel kapcsolatban megelőzte az Európai Uniót, hiszen a 2016. évi LXIX. tv.-nyel 2016. július 17. napjától kezdődő hatállyal egy szubszidiárius bűncselekményi alakzattal is kiegészítette a Btk.-t, azonban immáron annak nem a közbiztonság elleni bűncselekményeket tartalmazó fejezetében, hanem a köznyugalom elleni kriminalitásokat taglaló szerkezeti egységben. A Btk. fent nevezett módosítása a nagy nyilvánosság előtt elkövetett terrorizmus támogatására való uszítást, erre irányuló hírverés folytatását immáron önállóan is büntetni rendelte.[33] Ezen tényállás az elmúlt időszak terrorista akcióit, valamint azok elkövetőit tekintve különösen is indokolt. Több esetben is előfordult ugyanis, hogy a merénylő nem tartozott konkrétan valamely terrorszervezethez, azonban az elektronikus tömegtájékoztatási eszközök segítségével sugárzott propagandával egyetértve, a radikalizálódás irányába fordult, „hűségesküt téve" a szervezetnek.[34]

Fontos tehát leszögezni, hogy az ebben a tényállásban értékelt uszítás vagy hírverés folytatása nem egy konkrét terrorista támadáshoz, terrorcselekményhez kapcsolódik, de ilyen vagy ehhez hasonló szélsőséges magatartások megvalósításának a veszélyét egyértelműen magában hordozza. Azaz büntetendőségének nem feltétele, hogy ennek nyomán harmadik személyek ténylegesen is terrorista akciókat hajtsanak végre.[35] A tényállásban értékelt magatartás büntetni rendeltsége azért fontos, mert a radikalizálódás egyik eszköze lehet, ezért elengedhetetlen az ilyen magatartásokkal szembeni fellépés.

Éppen ezért az ilyen uszító cselekmények elsősorban a közbiztonságot és csak másodlagosan a köznyugalmat sértik. Véleményem szerint ezért az elsődleges jogi

[32] Erre maga az Irányelv is utal a 13. cikkben, amikor kimondja, hogy a büntetendőséget attól függetlenül biztosítani kell, hogy fennáll-e a kapcsolat az uszító magatartás és a terrorista bűncselekmény között.

[33] Lásd Btk. 331. § (2) bekezdés.

[34] Ilyenek voltak például a teljesség igénye nélkül az alábbi merényletek. 2017. április 7-én Stockholmban egy 39 éves férfi kerített a hatalmába egy teherautót, amit aztán a gyalogosforgalom felé irányított. 9 ember meghalt, és további 14 megsérült. Ez az elkövetési mód hasonló volt a 2017. március 22-i londoni merénylethez, ahol egy 52 éves férfi vezette az autóját a Westminster hídon a gyalogosok felé. A merényletben 5 ember meghalt, és legkevesebb 50-en megsérültek. Londonban ugyanebben az évben június 3-án volt hasonló akció a London hídon, ahol 8 ember meghalt, és további 48-an sérültek meg. A gyalogosforgalom ilyen formában történő veszélyeztetésével megvalósított merényletek közül 2017-ben a Barcelonában elkövetett volt a legsúlyosabb, amikor a merénylő augusztus 17-én a La Rambla sétányra hajtott be 15 ember halálát és további 131 ember sérülését okozva (Europol TE-SAT 2018. 23–24. o.).

[35] Neparáczki Anna Viktória: *A terrorizmus elleni fellépés eszközei a magyar és a német anyagi büntetőjogban.* PhD-értekezés. Pécs, 2017, 206. o.

tárgy okán indokoltabb lenne ezen tényállást a terrorcselekményhez kapcsolva egy önálló tényállásban a Btk. 318. §-a szerinti „Terrorizmus finanszírozása", valamint a Btk. 319. § szerinti „Értelmező rendelkezés" között elhelyezni „Terrorcselekmény elkövetésére irányuló uszítás" cím alatt. A cselekmény egyértelműen a terrorizmushoz kapcsolódó cselekmény, így a háborús uszítás tényállásán belüli szabályozásának nincs dogmatikai alapja.

Másodikként a nemzetközi szakirodalom alapján Dornfeld a *pénzgyűjtést* említi meg. A pénzgyűjtés természetesen a terrorszervezetek működése, a terrorizmus dinamikája szempontjából is nélkülözhetetlen eszköz. Ugyanakkor a terrorista célzatú forrásgyűjtés már régóta bűncselekménynek számít. Ezzel összefüggésben az Irányelv 11. cikke is leszögezi, hogy a terrorizmus finanszírozásán az olyan pénzgyűjtési tevékenységet érti, melynek célja valamely terrorista bűncselekmény vagy ehhez kapcsolódó büntetendő magatartás elkövetése, vagy az abban való bármilyen formájú közreműködés biztosítása. A terrorizmus pénzügyi támogatása a hatályos büntető anyagi jogunkban is kriminalizált magatartás, a cselekmény büntetendőségét a Btk. 318–318/A. §-ai biztosítják.[36]

Ugyanakkor kérdésként merül fel, hogy szükséges-e büntetőjogi eszközökkel reagálni az olyan magatartásokra, melyek a legális és illegális szálak összefűzött rendszerében egy-egy szervezet működését, fennmaradását általános szinten támogatják, ahhoz generális jelleggel járulnak hozzá. Másként feltéve a kérdést, szükséges-e a büntetni az olyan magatartásokat, melyek egy-egy szervezetet azok különféle „fedőszervezetein", „fedővállalkozásain" keresztül, a törvényes működés látszatának fenntartása érdekében támogatják? Hiszen ezekben az esetekben formálisan a „támogató" törvényesen folytatott tevékenységhez kapcsolódik.

Mivel mind az Irányelv, mind pedig a Btk. a finanszírozói magatartások esetében azok terrorcselekményhez vagy terrorista jellegű cselekményhez való kapcsolódását tényállási elemként határozzák meg – így a fentebb említett esetet alapvetően nem fedik le büntetőjogi válasszal, reakcióval –, a kérdés feltétele korántsem teoretikus. Az természetesen nyilvánvaló, hogy ha a támogató – például egy, az adott szervezethez kapcsolódó vállalkozás által nyújtott szolgáltatást igénybe vevő – személy nem tud arról, hogy az adott gazdálkodási tevékenység milyen mögöttes célokat szolgál, a bűnösségen alapuló felelősség elvéből is következően nem vonható felelősségre semmilyen bűncselekményért.

Amennyiben viszont szándékosan és abban a tudatban veszi igénybe és fizet egy szolgáltatásért, vagy fejt ki egyéb módon, támogatásként értékelhető magatartást, hogy az ő közreműködése révén keletkezett bevétel a későbbiekben milyen célokra kerülhet felhasználásra, közvetve alapvetően a terrorista szervezet fennmaradásához

[36] A terrorizmus finanszírozása elleni fellépés szükségessége az Irányelv 11. cikkén alapszik. A hazai Btk. hatályos szövegét 2018. január 1-i hatálybalépési időponttal a 2017. évi XXXIX. törvény alakította ki.

járul hozzá. Viszont mivel nincs kapcsolata, ismerete konkrét terrorista támadásról vagy terrorista jellegű bűncselekményről és ahhoz kapcsolódó személyről, így magatartása nem illeszthető be a Btk. említett rendelkezéseibe. Ez tehát egy szürke folt. Egy olyan határvonal a terrorizmus elleni fellépés anyagi jogi szabályozásában, mely mindenképpen megoldandó feladat, ugyanakkor belátom, hogy egy ilyen tényállás absztrakciója korántsem egyszerű jogalkotói munka.[37]

A harmadik, fentiekben említett terület az *információ terjesztése.* Természetes, hogy a terjesztett információ sokféle lehet, több mindenre is vonatkozhat, ugyanakkor Dornfeld hivatkozott tanulmánya nyomán egy dologban mindenképpen különbözik a propagandától. Nevezetesen ebben az esetben a terroristák saját, már meglévő szimpatizánsaikkal kívánnak információkat megosztani,[38] például egy konkrét terrorista akcióról, annak végrehajtásáról, következményeiről. Ebben az esetben az internet tehát valamiféle hírforrás a szervezet tagjai számára. Ez a tömegtájékoztatás mindaddig, amíg már nem fordul át propagandává, álláspontom szerint nem éri el azt a küszöböt, amelyet a büntetendőség körében akár az Irányelv, akár a hazai Btk. felállított. Az pedig, hogy a híradások átfordulnak-e propagandává, azt minden esetben az adott híradás tartalma, kimutatható hatásai alapján kell és lehet is megítélni, eseti jelleggel, az eset összes körülményének mérlegelése révén.

A terjesztett információ ugyanakkor akár ismeretterjesztő célokat is szolgálhat, mely nemcsak a terrorista szervezetek követőinek számaránybeli növekedéséhez, de akár a terrorista akciók végrehajtásához szükséges ismeretek megszerzéséhez, azok elmélyítéséhez is hozzájárulhat. Az Irányelv éppen ennek megakadályozása céljából mind a toborzói, mind pedig a kiképzéshez közreműködőként kapcsolódó magatartásokkal szemben a szükséges büntetőjogi válaszok megfogalmazására hívta fel az egyes tagállamokat.[39] A dogmatikai problémát ugyanakkor az olyan információk, ismeretek közvetítése, átadása jelenti, melyek esetében azok nem kapcsolódnak egy

[37] Belátható ugyanis dogmatikai szempontból, hogy egy ilyen magatartás a jelzett indokok miatt nemcsak a terrorizmus finanszírozása, sem pedig a bűnszervezetben részvétel mint sui generis előkészületszerű bűncselekmény törvényi tényállásába nem illeszthető. Utóbbi esetében a terrorista csoport és a bűnszervezet legáldefiníciójában rejlő különbségek is minősítési problémát jelenthetnek.

[38] Dornfeld: i. m. (2019), 54. o.

[39] Az Irányelv 6. cikke, valamint 15. cikk (4) bekezdése előírja, hogy a tagállamok nyilvánítsák büntetendő magatartásnak a terrorista bűncselekmény elkövetésére, vagy az abban való közreműködésre történő felhívást, kiemelten akkor is, ha a célszemélyek gyermekkorúak. A kiképzéssel kapcsolatos 7. cikk tekintetében ugyanezt az elvárást fogalmazza meg az Irányelv. Bár az Irányelv és annak magyar fordítása is a 6. cikk tekintetében a „felhívás"-ban jelöli meg az elkövetési magatartást, látva a preambulumban is rögzített célokat nyilvánvalóan az eredményes és az eredménytelen felbujtás is egyaránt üldözni kívánt magatartás az Irányelv szellemiségét tekintve. Lásd ezzel kapcsolatban: Bartkó Róbert: Az Unió 2017/541. sz. Irányelvének hatása a V4 országainak büntető anyagi jogszabályalkotására. In Bartkó Róbert (szerk.): *A terrorizmus elleni küzdelem aktuális kérdései a XXI. században.* Budapest, Gondolat Kiadó, 2019, 145. o.

konkrét terrorista bűncselekményhez.[40] Ez ismételten egy olyan „szürke folt", ahol a jogalkotásnak igazodnia kellene az uniós követelményekhez. A problémát jelentő esetek ugyanis pont az olyan ismeretterjesztésre vonatkoznak, melyek közép- vagy akár rövid távon is terrorista akciók megjelenéséhez, elkövetéséhez vezethetnek, azonban közvetlen terrorista célzatuk hiányában nem illeszthetők be egyik terrorizmushoz kapcsolódó tényállásba sem. Hasonlóan a pénzgyűjtési célzatnál említettekhez, egy ilyen tényállás absztrakciója is komoly kihívás nemcsak a jogalkotás, de a jogalkalmazás számára is, hiszen számtalan bizonyítási nehézséget hordoz magában.

A negyedik és egyben utolsó terrorista internethasználati cél *a biztonságos kommunikáció és a hírszerzés*. A terrorizmus dinamikája szempontjából nemcsak a folyamatos pénzügyi ellátottságnak, de természetesen – minthogy a bűnözés egyik formájáról van szó – az információkkal való rendelkezésnek is jelentős szerepe van. A terroristák igyekeznek az internet olyan felületeit használni, ahol az egymás közötti kommunikáció, a társadalom adott szegmensébe alvó sejtként beépült alegységek tagjai által megszerzett információk titkosan, a bűnüldöző hatóságok előtt láthatatlan módon tudnak gazdát cserélni.

Az anonimitás ezen a területen különösen is fontos, melyet a terroristák is – más bűnözői csoportokhoz hasonlóan – a különféle információtechnológiai megoldások használatával tudnak elérni. Így például nagy segítséget jelentenek a terroristák számára is a kiberbűnözők által is igénybe vett privát szférát erősítő technológiák, mint például „a virtuális magánhálózatok (VPN), melyek segítségével a felhasználó könnyedén kaphat a világ bármely más országába mutató IP címet"[41] is.

Ezeknek a csatornáknak tehát elsődlegesen az adott terrorista akció előkészítése során van komoly szerepe, melyek az Irányelvvel való összhangban sui generis tényállásban értékelt büntetendő magatartások a hatályos Btk.-ban. Amennyiben a terroristák közötti kommunikáció tartalma szerint nem kapcsolható konkrét akcióhoz, a büntetőjog által értékelési körön kívül marad, ugyanakkor az egyes szervezetek, vagy azok sejtjei, illetve az egyes elkövetőkkel szembeni titkosszolgálati eszközöket is igénybe vevő felderítési munkában fontos szerepük van, hiszen ezek feltérképezése révén lehetnek képesek a hatóságok egy-egy akciót meghiúsítani, egy-egy szervezetet, csoportot vagy alvó ügynököt kézre keríteni.

[40] Az Irányelv 13. cikke értelmében: „a terrorista bűncselekmény tényleges elkövetése nem szükséges feltétele annak, hogy a 4. cikkben vagy a III. címben említett bűncselekmények büntetendőnek minősüljenek, az 5–10. és a 12. cikkben említett bűncselekmények büntetendővé minősítésének szempontjából pedig szintén nem tekinthető szükséges feltételnek az ebben az irányelvben meghatározott valamely más konkrét bűncselekmény vonatkozásában fennálló kapcsolat megállapítása."

[41] Dornfeld: i. m. (2019), 55. o.

3. TERRORIZMUS FINANSZÍROZÁSA A KIBERTÉRBEN

A terrorista csoportok akkor tudnak hatékony romboló tevékenységet kifejteni, ha létrehoznak bizonyos szervezeti struktúrákat. Ezek a szervezeti keretek egyébként kísértetiesen hasonlítanak az üzleti szervezetek által kialakított szervezeti és működési formákhoz.

Két ideális szervezeti forma létezik, amelyet a terroristák használhatnak:

1. a parancsnok-beosztott típusú, vagyis *hierarchikus szervezet;*
2. *a hálózati típus.*

Napjainkban a terrorszervezeteknek aktív adaptációs mechanizmussal kell reagálnia a környezeti változásokra, vagyis arra, hogy a jogi szabályozás következtében folyamatos külső nyomás nehezedik rájuk. Emiatt *a hálózati típusú szervezeti forma a hatékonyabb.* A terroristák virtuális hálózatokat hoznak létre, ahol a részt vevő terrorista sejtek legtöbbször a saját maguk által biztosított forrásokból finanszírozzák a működésüket, kapcsolatuk a központtal nagyon laza. A vezető feladata csak az, hogy világképet és ideológiát szolgáltat, és stratégiákat javasol, ezt azonban soha nem konkrét csoporttagoknak, hanem csak úgy általánosságban. A vezető feladata inkább az ösztönzés, nem a parancsolás. A virtuális hálózat előnyei a terroristák számára:

a) a funkciók megtöbbszöröződése, vagyis a redundancia (így erősebbé válnak a külső behatásokkal szemben, és egy sejt vagy csoport kiesése esetén nem omlik össze az egész hálózat, hasonlóan az internet felépítésének alapfilozófiájához[42]);
b) az internet szerepe: virtuális terrorista közösségek alakulhatnak;
c) a tagok, az egyes terroristák és terrorista sejtek személyes találkozás nélkül kommunikálhatnak egymással a kibertéren keresztül;
d) a minimális kommunikáció rendkívül nehéz az ilyen szervezetekbe beépülni.

A virtuális hálózat azonban egy komoly hátrányt is rejt magában: az ilyen terrorszervezetek nem vagy csak nagyon nehezen képesek komplex feladatok megoldására. Erre a célra inkább a hierarchikus, parancsnok-beosztott típusú szervezet alkalmas. A hierarchikus felépítésű terrorszervezetek azonban sebezhetőbbek, ezért szinte kizárólag csak olyan államokban tudnak működni, amelyiknek a központi kormányzata gyenge. A CIA becslése szerint jelenleg hozzávetőlegesen 50 ilyen államot találunk, ezek közel felében működnek hierarchikus szervezeti struktúrával rendelkező

[42] A hatvanas évek végén merült föl az USA-ban egy kevéssé sebezhető számítógép-hálózat szükségessége, amelynek egy esetleges atomtámadás után megmaradó részei működőképesek maradnak. Ezen az elven kezdett működni 1969-ben az ARPANET, amelyből a polgári változat, az internet 1983-ban kiválva megszületett.

terrorista csoportok. (Az al-Káida hierarchikus felépítésű központi magja vélhetően Pakisztán törzsi uralom alatt álló területein rejtőzik.[43])

Elmondhatjuk tehát, hogy a 21. században új típusú terrorfenyegetettséggel kell szembenéznünk: a „war on terror" politikája, amit az USA meghirdetett, aktivált egy kevésbé lazán összekapcsolódó, dzsihádista sejtekből álló, globális terrorista hálózatot... Emellett az is aggodalomra adhat okot, hogy egyes szakértők szerint az elsődleges terrorista célpontok ma már az európai nagyvárosok.[44] Ezt számos terrortámadás támasztja alá az elmúlt évtizedből.

A terrorszervezetek mindkét alaptípusa legalább egy tekintetben megegyezik: anyagi erőforrásokra van szüksége a támadások megszervezéséhez és végrehajtásához. Ez a számukra költségként jelentkezik. Érdemes megvizsgálni a terrorizmus költségeit két oldalról: a terroristák oldaláról (finanszírozási igény) és a társadalom oldaláról (károk és áldozatok).

A terrorizmus finanszírozása azt a tevékenységet jelenti, amelynek során közvetve vagy közvetlenül terrortámadások megvalósításához anyagi eszközöket bocsátanak rendelkezésre. *A terrorizmusnak a témánk szempontjából talán a legfontosabb jellemvonása az, hogy nem szükséges nagy összeg az egyes akciók kivitelezéséhez.*

A költségek három nagy csoportja: a műveleti költségek, az adminisztratív költségek és a merénylők családtagjainak adott dotáció.

Néhány példa a „műveleti költségek"-re:

- 1993. február 26-án a World Trade Center ellen egy gépjárműben elrejtett, 680 kg súlyú bombával követtek el merényletet, ennek költsége 18 000 USD volt, 6-an meghaltak, és több mint 1000 sebesült volt,
- a 2001. szeptember 11-i, a világtörténelem eddigi legnagyobb, csaknem háromezer emberáldozatot követelő terrortámadásának összköltsége a becslések szerint 4-500 000 USD volt, ebből 300 000 USD érkezett banki átutalások formájában,
- a 2002. október 12-én végrehajtott bali robbantás becsült bekerülési költsége 20-35 000 USD volt, 190 halott és 309 sebesült volt a mérleg másik oldalán,
- a 2003. november 15-én és 20-án Isztambulban végrehajtott pokolgépes akciók 40 000 USD körüli összegbe kerültek, 27 halott és 450 sebesült maradt a helyszínen,
- 2004. március 11-én Madridban robbantak bombák, ezt az akciót 10 000 (spanyol becslések szerint 60 000) USD költségvetéssel tudták a merénylők kivitelezni; a mérleg másik oldalán 191 halott és több mint 1500 sebesült volt,
- 2004. november 2-án megkéselték és lelőtték Theo Van Gogh holland filmrendezőt, akit az iszlámról vallott radikális nézetei miatt korábban már többször

[43] Thomas J. Bierstecker – Sue E. Eckert (szerk.): *Countering th Financing of Terrorism.* London, New York, 2008, 23–27. o.

[44] Sean S. Costigan – David Gold: *Terronomics ASHGATE.* Printed in Great Britain, 2007, 19. o.

megfenyegettek. Ugyan ebben az esetben „csak" egy halálos áldozattal járt a támadás, de a költsége elképesztően alacsony: 100 USD volt!
- 2005. július 7-én Londont érte támadás, 700-an megsérültek, 38-an életüket vesztették. A támadás teljes költsége mindössze 15 000 USD volt.

Látható tehát, hogy a terrortámadások kivitelezése elképesztően alacsony költségvetéssel is megoldható, az okozott károk viszont óriásiak. Ezekből az összegekből azt a következtetést is levonhatnánk, hogy a terrorizmus finanszírozása elleni küzdelemnek nincs sok értelme. Ez így nem igaz. Nagyon nehéz feladat a terroristákat elvágni a pénzügyi forrásaiktól, de nem lehetetlen, és van értelme az erre irányuló erőfeszítéseknek. Erre két példát hoznék fel igazolásképpen:

1. Az 1993-as WTC elleni merénylet után az egyik elfogott elkövető, Ramzi Yousef bevallotta, hogy nagyobb bombát akartak használni, de nem volt rá pénzük! Ráadásul a nyomozásban az egyik kulcselem az volt, hogy a terroristák vissza akartak kapni egy letéti díjat, amit a merényletet megelőzően a robbantáshoz használt furgonért fizettek…[45]
2. A terrorszervezetek működési költsége sokkal nagyobb, mint az egyes műveletek végrehajtási költsége. Az a terrorszervezet, amelyik nem jut kellő mennyiségű anyagi erőforráshoz, lassan elsorvad.

A második költségtényező az adminisztratív, vagyis a működési költség. Az al-Káida például a bevételeinek kb. 10%-át költi műveleti költségekre, 90%-ot a szervezet adminisztratív és működési költségeire fordít.[46] A finanszírozási igény természetesen függvénye a szervezeti struktúrának. A hierarchikus szervezet magasabb finanszírozási igényével szemben a hálózati struktúra lényegesen kevesebb pénzből is működtethető. Ha ehhez még azt is hozzátesszük, hogy a virtuális hálózat egyes elemeit alkotó terrorista sejtek sokszor önfinanszírozó módon működnek, akkor komoly aggodalmaink támadhatnak. Rögtön meg kell jegyeznünk azonban, hogy egy önfinanszírozó terrorista sejtekből álló virtuális hálózati struktúrában működtetett terrorszervezet lényegesen veszít a hatékonyságából a hierarchikus struktúrához képest, és gyakorlatilag nem tud összehangolt, valamint egyáltalán nem tud nemzetközi méretű műveleteket végrehajtani.

Ennek ellenére – ahogy Donald Rumsfeld fogalmazott – „A költség-haszon arány ellenünk dolgozik! A mi milliárdos költségeink állnak szemben a terroristák milliós költségeivel."[47]

[45] Bierstecker–Eckert: i. m. (2008), 7. o.

[46] D. Bugg: Speech to IAP Conference 8. 12. 2003. (http://www.cdpp.gov.au/Media/Speeches/20030812db.aspx).

[47] http://www.globalsecurity.org/military/library/policy/dod/rumsfeld-d20031016sdemo.htm.

Van a terrorista támadásoknak egy érdekes, új költségtényezője is, ez az öngyilkos merénylők családtagjainak – általában egy összegben – fizetett anyagi dotáció, illetve életjáradék. Ez a Hamász esetében becslések szerint 5000 USD, de például Szaddám Huszein regnálása során 25 000 USD-t ajánlott az öngyilkos merénylőknek „sikerdíjként".[48] Ez azonban nem növeli meg jelentősen a terrorista támadások költségét, mivel:

1. az öngyilkos merénylők egy jelentős része gazdag (vagy legalábbis jó körülmények között élő) családból származik, így ezek esetében nincs jelentős szerepe az anyagi ösztönzésnek,
2. a „sikerdíj" nem minden esetben a terrorszervezet vagy terrorista sejt költségvetését terheli, mint ahogy ezt Szaddám Huszein példája is mutatja.

A terrorista támadások kivitelezésének összköltsége tehát napjainkban három alapvető költségtényező nagyságától függ: a terrorszervezet adminisztratív, fenntartási költségei[49], az öngyilkos merénylő családjának juttatott anyagi támogatás[50], valamint a terrortámadás végrehajtásának közvetlen operatív költségei.[51]

A terrorizmus finanszírozásának a legtágabb értelemben négy fő formája ismert:[52] bűncselekmények elkövetése, adományok, törvényes üzleti tevékenység és meghatározott földrajzi területi egységek feletti kontroll.

1. Bűncselekmények elkövetése

A terrorizmus a bűnözés egyik formája, mégpedig az egyik legsúlyosabb és legveszélyesebb formája. Emiatt a terrorszervezetek természetszerűen nem riadnak vissza attól, hogy egyéb bűncselekményeket is elkövessenek. Ennek a kockázata általában kisebb is, mint a terrorcselekményé, hiszen a büntetési tételek rendszerint alacsonyabbak. A terroristák általában olyan bűncselekménytípusokat kedvelnek, amelyek rövid idő alatt nagy összegű bevételt eredményeznek.

Talán a legkedveltebb ezek közül is *kábítószerrel visszaélés*. A kábítószer-kereskedelem adja a kolumbiai paramilitáris szervezetek és gerillák bevételeinek 60-90%-át.[53] Az iszlám terrorista szervezeteket ráadásul néhány fatva kifejezetten fel-

[48] Bierstecker–Eckert: i. m. (2008), 102. o.

[49] Ez a szervezet nagyságától függ, sokszor kis terrorista sejtek alacsony működési költségek mellett is képesek nagy károkat okozó merényletek végrehajtására, ugyanakkor a nemzetközi ütőképességük minimális.

[50] Ennek a mértéke különböző, és természetesen (szerencsére) nem minden támadásban vesznek részt öngyilkos merénylők.

[51] Sajnos ez a legkisebb költségtényező, pedig jórészt ezen múlik az akció sikeressége, illetve az okozott kár nagysága is.

[52] Lásd Gál István László: *A terrorizmus finanszírozása. Die Terrorismusfinanzierung.* Pécs, Pécsi Tudományegyetem Állam- és Jogtudományi Kar Gazdasági Büntetőjogi Kutatóintézet Pécs, 2010.

[53] Berry, L. V. – Curtis, G. E. – Hudson, R. A. – Kollars, N. A.: *A Global Overview of Narcotics-Funded Terrorist and Other Extremist Groups.* Library of Congress 2002. 52. o.

hatalmazza arra, hogy a dekadens Nyugattal szemben folytatott küzdelmükben a kábítószer-kereskedelmet eszközként használják fel.[54]

Emellett a terroristák jelentős bevételforrása az *emberrablás* is. Az IMU (Üzbég Iszlám Mozgalom) például 5 millió USD bevételhez jutott négy japán geológus szabadon engedéséért cserébe, miután 1999-ben elrabolták őket Kirgizisztánban.[55]

Az *embercsempészet* is jövedelmező tevékenység a terroristák számára. A világ fejletlen és fejlett régiói közötti életminőség-különbség, illetve a demokratikus államok által nyújtott biztonság iránti vágy hívta életre a gazdasági és a politikai migrációt. Ahhoz, hogy egy bangladesi vagy egy kínai állampolgár eljusson Nyugat-Európába, 20-25 ezer dollárt is kell áldoznia.[56]

A *pénzmosás* egyrészt jövedelmező tevékenység a terroristák számára, így tehát a terrorizmus finanszírozásának az egyik eszköze is. Másrészt viszont rokon jelenségnek is tekinti a szakirodalom tekintélyes része a terrorizmus finanszírozását és a pénzmosást. A terrorizmus finanszírozása várhatóan rövid időn belül mint „fordított pénzmosás" vagy „pénzbepiszkítás" (money dirtying) be fog épülni a tágabb értelemben vett pénzmosásfogalomba is. A terrorizmus finanszírozása viszont a pénzmosással összehasonlítva a következő eltérő jellemvonásokkal rendelkezik:[57]

- A motívum inkább erőszakos (megfélemlítés), mint anyagi (nyereségvágy). A terroristák célja leginkább állami szervek, nemzetközi szervezetek valamire történő kényszerítése, a lakosság megfélemlítése vagy más állam alkotmányos, társadalmi vagy gazdasági rendjének megváltoztatása, illetve megzavarása. Ezeket a nemzetközi dokumentumok által megnevezett célokat a magyar Btk. is tartalmazza a terrorcselekményről szóló 261. §-ban. A terroristák célja tehát csak a legritkább esetben lehet a haszonszerzés, míg a pénzmosók egyértelműen „profitorientáltak".
- A terrorizmus finanszírozására ugyanúgy felhasználnak legális forrásból származó pénzt, mint illegálisat. A terroristák a pénzügyi támogatásként kapott összeg jelentős részét olyan legális forrásból kapják, mint például a karitatív szervezetek, jótékony adományozók, illetve törvényesen működő cégek.
- A harmadik megkülönböztető jellemvonás az eltérő összegnagyság. A nagyobb terrortámadások is megszervezhetők és lebonyolíthatók viszonylag kisebb összegekből is. A 2001. évi New York-i repülőgép-eltérítések elkövetői például külföldi diáknak álcázva szerény támogatási összegeket vettek fel rendszeresen, és kivétel nélkül egyik átutalás sem érte el a „bűvös" 10 000 dolláros határt.

[54] Beers, R. – Taylors, F. X.: Narco-Terror: The Worldwide Connection Between Drugs and Terror. *Terrorsim and Goverment Information*, 2002, 322. o.

[55] Napoleoni, L.: *Modern Jihad: Tracing the Dollars Behind the Terror Networks*. London, Pluto Press, 2003, 89. o.

[56] Korinek: i. m. (2006), 456. o.

[57] Steven Mark Levy: *Federal Money Laundering Regulation (Banking, Corporate, and Securities Compliance)*. New York, 2003, 2. fejezet 18–20. o.

Emellett vannak még *egyéb* jövedelmező bűncselekménytípusok is, amelyeket a terroristák felhasználnak a pénzszerzésre. Ezek taxatív felsorolása lehetetlen. 2002-ben az IRA állítólag 11 millió USD bevételhez jutott különféle bűncselekmények elkövetése révén. A bevételük legnagyobb része Kelet-Európából Angliába irányuló dohánycsempészetből származott.[58] Az al-Káida európai pénzügyi bevételeinek a nagy része pedig hitelkártyacsalásokból származik, titkosszolgálati becslések szerint ez az összeg eléri az 1 millió USD-t havonta (!).[59]

2. Adományok

Az adomány készpénz, számlapénz, értékpapír, nemesfémek, drágakövek vagy egyéb, értékkel rendelkező forgalomképes vagyontárgyak ingyenes, ellenszolgáltatás nélküli átadása terroristák vagy terrorista szervezetek részére. Tipikus formája a pénzbeli támogatás. A terroristák egyébként a legmagasabb likviditási fokkal rendelkező vagyontartási formát, a készpénzt részesítik előnyben.

A terroristákat támogathatják magánszemélyek, szervezetek (akár más terrorszervezetek is) és államok. A tágabb értelemben vett „adomány" tekinthető a terrorizmus finanszírozásának büntetőjogi értelemben, míg közgazdasági értelemben a bűncselekmények elkövetése és a legális üzleti tevékenység is e tevékenység része.

Szűkebb értelemben terrorizmus finanszírozása elleni büntetőjogi szabályozás elsődlegesen a magánszemélyek adományaira fókuszál, ha államok támogatnak terrorista célokat, az sokszor megoldhatatlan probléma elé állítja a büntetőjogot. Nem mindegy ugyanis, hogy az állami dotáció milyen formában (közvetlen vagy közvetett pénzügyi juttatás), milyen fedéssel (kereskedelmi ügylet, humanitárius segítség stb.) és milyen katonai-gazdasági erővel rendelkező államtól (kis ország, nagyobb, esetleg atomfegyverrel is rendelkező állam vagy esetleg egy szuperhatalom) származik.

3. Törvényes üzleti tevékenység

Oszáma bin Láden Szudánban 30 céget alapított 1991–1996 között, ezeknek összesen 3000 alkalmazottja volt. Már 1994–1995-ben nyugati és izraeli titkosszolgálati források úgy emlegették bin Ládent, mint a terrorizmus kulcsfinanszírozóját.

A törvényes üzleti tevékenység egyre fontosabb szerepet játszik a terrorizmus finanszírozásában, mint ahogy általános értelemben az is kijelenthető, hogy a terrorizmus finanszírozásában egyre fontosabb szerepe van a legális forrásoknak. Említettük már, hogy főként az európai dzsihádista sejtek egyre inkább támaszkodnak legális bevételeikre, például arra, amit törvényes munkahelyükön keresnek meg. A szeptember 11-i támadás volt az utolsó merénylet, amelyet az al-Káida finan-

[58] Clarke, L. – Leppard, D.: Photos link more IRA Men to Colombia. *Sunday Times*, 2002.

[59] Gunaratna, R.: *Inside Al Quaeda: Global Network of Terror*. London, Hurst & Company, 2002. 65. o.

szírozott teljes egészében, 2002-ben a globális finanszírozás megszűnt! A mai robbantások döntő többsége önfinanszírozó sejtek akciója. Megindult tehát egy olyan folyamat, amelyet a *terrorizmus finanszírozása privatizációjának* nevezett el a szakirodalom.[60]

A törvényes üzleti tevékenység részének tekinthető tágabb értelemben az is, ha a terroristák munkavállalóként a legális jövedelmük egy részét használják fel terrorista célokra. Ha abból indulunk ki, hogy az elmúlt évek nagyobb terrortámadásainak tapasztalatai alapján 8-10 000 USD összegből már komoly akció kivitelezhető, akkor reális lehet azon félelmünk, hogy egy négy-öt fős terrorista sejt két-három év alatt gyakorlatilag bármelyik fejlett vagy közepesen fejlett országban, bármilyen legális munkával meg tud takarítani egy ekkora összeget,[61] és képes csapást mérni anélkül, hogy szüksége lenne bármilyen egyéb addicionális forrásra!

4. Meghatározott földrajzi területi egységek feletti kontroll[62]

A terroristák úgy is juthatnak finanszírozási forrásokhoz, ha kvázi államként kezdenek működni egy meghatározott területen, ennek keretében pedig hasonló módon tesznek szert bevételekre, mint a nemzetközi közösség tagjaiként elismert államok. Adót szednek, kereskednek, pénzügyi műveleteket végeznek, stb. Erre a legjobb példa az Iszlám Állam néven hírhedtté vált terrorszervezet volt.

A terrorizmus finanszírozása az online térben részben hasonló, részben pedig különbözik a fentebb bemutatott hagyományos finanszírozási formáitól. Az online térben megfigyelhető terrorizmusfinanszírozási technikákat Serbakov munkája[63] alapján a következő csoportokra oszthatjuk:

1. Terrorizmusfinanszírozás online kiskereskedők és piacok használatával

2. Adománygyűjtés és közösségi finanszírozás a közösségi médián

2.1. Új fizetési termékek és szolgáltatások

2.2. Virtuális fizetőeszközök

2.3. Internetes pénzügyi szolgáltatások

Ad 1. A terroristák a legnagyobb online kereskedelmi piactereket (például Amazon, eBay, Alibaba) felhasználva is igyekeznek finanszírozási forrásokat előteremteni a közvetlen műveleti költségeik, valamint a terrorszervezet működtetésének adminisztratív költségei számára. Több forrás is megerősíti, hogy az Iszlám Állam a működési területén zsákmányolt antik műkincseket online kereskedelmi piacte-

[60] Sean S. Costigan – David Gold: *Terronomics ASHGATE.* Printed in Great Britain, 2007, 14. o.

[61] Ötfős sejttel számolva két év alatt 10 000 USD megtakarításához elég, ha személyenként egy év alatt 1000 USD a megtakarítás összege. Ez alig több, mint 80 USD havonta.

[62] Sieber–Vogel: *Terrorismusfinanzierung: Prävention im Spannungsfeld von internationalen Vorgaben und nationalem Tatstrafrecht.* Berlin, Duncker & Humblot, 2015, 10. o.

[63] Serbakov Márton Tibor: *Egyes szélsőséges terrorista csoportok internethasználata egyes aspektusainak elemzése.* PhD-értekezés. Pécs, Pécsi Tudományegyetem, 2022, 84–99. o.

reken értékesítette.[64] Ez gyakorlatilag az Ulrich Sieber által leírt negyedik hagyományos terrorizmusfinanszírozási technika körébe sorolható online módszer.

Ad 2. A terroristák a 21. században már a közösségi médiát is felhasználják arra, hogy forrásokat gyűjtsenek. Erre akár a Facebook különösen jó lehetőséget jelent, de például a kínai WeChat alkalmazás, ami egyben afféle közösségi médium és üzenetküldő, illetve kommunikációs alkalmazás is, fizetőeszközként és pénzátutalási applikációként is használható. Napjainkban a WeChat az egyik legnépszerűbb fizetési csatorna Kínában az Alipay mellett. Ez a Kínában élők és a külföldiek számára is rendelkezésre áll, mivel a WeChat fiók létrehozásához nincs szükség kínai személyi igazolványra. Ezenkívül az út menti árusoktól a nagy bevásárlóközpontokig mindenki elfogadja a WeChattel történő fizetést, megkönnyítve a mindennapi életet. Bárki könnyedén átutalhat pénzt WeChat-fiókjából bármelyik ismerőse fiókjába.[65] Ez a platform tehát a terroristák és más bűnözők számára is alternatívát jelenthet, bár a tranzakciók nem teljesen anonimek, de kisebb összegek esetén nagy valószínűséggel nehezen felderíthetők a hatalmas volumen miatt. Serbakov egy példát is leír a terrorfinanszírozás ezen változatára: „Példa egy hatóságok előtt ismert terrorizmus finanszírozó és családja megsegítésére indított közösségi finanszírozásra: »A« személyt 2016-ban terrorizmus finanszírozásával vádolták meg. Egy GoFundMe közösségi finanszírozás kampányt hoztak létre e személy és terhes felesége támogatására. A támogatandó ügy leírása a következő volt: »Nemrég egy testvér aseer (fogoly) lett a tawagheet (hitetlenek) kezében. (Recently a brother has become an aseer (prisoner) at the hands of the tawagheet (nonbelievers).« A kampány két nap alatt 3000 USD összeget hozott."[66]

Mindezek mellett komoly biztonsági kockázatot rejt magában az is, hogy új fizetési termékek és technológiák jelentek meg az interneten a 21. században. A kriptovaluták különösen alkalmasak a terrorizmus finanszírozására, pénzmosásra, illegális fegyverkereskedelemre és egyéb bűncselekmények finanszírozására, elkövetésük megkönnyítésére, ugyanis ezek „jogi státusza jellemzően nem eldöntött az egyes jogrendszerek esetében. Az az álláspont kezd kirajzolódni, hogy amennyiben értékpapírnak minősül a kriptoérme-kibocsátás, akkor kötelező nemcsak az értékpapír-kibocsátásra vonatkozó jogi szabályozás, de tőzsdei bevezetést követően az értékpapírok tőzsdei bevezetésére vonatkozó szabályok betartása is. Így egy értékpapír-minősítés kifejezetten versenyhátrányt jelent a többi kriptovalutához képest azon kriptoérme kibocsátójának, aki ezt a minősítést megkapta, azzal szemben, aki által a kibocsátott kriptovaluta nem

[64] Vö. Jessica Davis: *New Technologies but Old Methods in Terrorism Financing.* London, Royal United Services Institute for Defence and Security Studies, 2020.

[65] https://www.webnots.com/how-to-do-money-transfer-in-wechat-accounts/.

[66] *Social Media And Terrorism Financing.* APG/MENAFATF, Sydney South, 2019. 12. o. (http://www.apgml.org/methods-and-trends/news/details.aspx?pcPage=1&n=1142); alapján Serbakov: i. m. (2022), 86. o.

értékpapírként kerül meghatározásra."[67] 2021. január 1-től a magyar Btk. egyik módosítása a pénzmosás tényállása mellett annak elkövetési tárgyát is megváltoztatta, pont azért (a jogszabály indokolása szerint is), hogy például a tokenek és más hasonló aktívák bevonhatók legyenek ebbe a körbe, elkövethető legyen rájuk a bűncselekmény. Valamint rámutatnak a szerzők, hogy a „kriptovaluták kibocsátásának és tőzsdei kereskedésének a szabályozása és felügyelete éppen azok határterületi elhelyezkedése miatt jelent komoly kihívást a szabályozó hatóságok számára".[68] Manapság számos „online fizetési rendszer és digitális fizetőeszköz anonim, ami vonzóvá teszi őket a terrorizmus finanszírozása szempontjából, különösen akkor, ha a fizetési rendszer egy viszonylag gyengébb pénzmosás/terrorizmus finanszírozás elleni rezsimű joghatóságban működik. A virtuális fizetőeszközök komoly pénzügyi innovációs lehetőséget jelentenek, de számos bűnözői csoport figyelmét is felkeltették, és terrorizmus finanszírozási kockázatot jelenthetnek."[69]

A kriptovaluták és más virtuális fizetőeszközök lényegében elektronikus pénzként viselkednek, nem derivatív eszközökként. „A derivatív termék olyan pénzügyi szerződés, amelynek értéke az alapul szolgáló piaci tényezők, például kamatlábak, valutaárfolyamok és árucikkek, hitel- és részvényárak teljesítményéből származik. A származékos ügyletek a pénzügyi szerződések széles választékát foglalják magukban, beleértve strukturált adósságkötelezettségeket és betéteket, swapokat, határidős ügyleteket, opciókat, fedezeti ügyleteket és ezek különféle kombinációit"[70] – olvasható The Office of the Comptroller of the Currency (OCC) honlapján, amely a U. S. Department of the Treasury egyik szervezete. Vagyis derivatívák csak olyan pénzügyi szerződések lehetnek, amelyek árfolyama egy másik eszköz árfolyamához kötött. Sem a definícióban, sem a hozzá kapcsolódó egyéb elemzésekben nem szerepel, hogy egy elektronikus pénz derivatív eszköznek tekinthető. A származékos ügyletek (derivatívák) egyik legfontosabb jellemzője a szakirodalom szerint az, hogy jelentős hitelmennyiség található mögöttük, vagyis egyik fő jellemzőjük a tőkeáttétel. „Látható tehát a fentiekből, hogy a származtatott ügyletekben hatalmas mennyiségű hitel található, ami gyakorlatilag a kötvény, részvény, árupiaci termékek piacán kötött ki."[71] A derivatívák fajtái:

- CFD[72]-termékek (index, futures, részvény CFD);
- határidős piaci termékek;

[67] Kecskés András – Halász Vendel – Bujtár Zsolt: *Tőzsdeuniverzum.* Budapest, HVG-ORAC Kiadó, 2019, 220. o.

[68] Kecskés–Halász–Bujtár: i. m. (2019), 224. o.

[69] Serbakov: i. m. (2022), 87. o.

[70] https://www.occ.treas.gov/topics/supervision-and-examination/capital-markets/financial-markets/derivatives/index-derivatives.html.

[71] https://elemzeskozpont.hu/szarmaztatott-ugylet-derivativa-jelentese-fogalma-mik-azok

[72] A CFD az olyan instrumentumokat foglalja magában, amelyeket a nyitó és záró értékek közti különbséggel kereskednek.

- opciós termékek;
- deviza forward ügyletek;
- certifikátok, warrantok.[73]

Az elektronikus pénzek, illetve a készpénz-helyettesítő fizetési eszközök mögött értelemszerűen nem áll hitel, a derivatíváknak pedig éppen ez az egyik legfontosabb jellemzője. Az elektronikus pénzek tehát emiatt terrorizmusfinanszírozására és bármilyen más illegális tevékenységre (például pénzmosás elkövetésére) könnyebben felhasználhatók, mint a derivatív eszközök vagy egyéb hagyományos pénzügyi termékek, nem is említve az azonosításhoz kötött bankszámlákat.

Végül az internetes pénzügyi szolgáltatások is felhasználhatók online terrorizmus finanszírozására és más bűncselekmények elkövetésére egyaránt. „Az előre feltöltött számlák, melyeket online árverési fizetésekhez használnak, a legdominánsabb internetes pénzügyi szolgáltatásokhoz tartoznak. Előfordulhat, hogy a kedvezményezetteknek regisztrálniuk kell a pénzforgalmi szolgáltatónál, hogy átutalást kapjanak. Néhány olyan online fizetési rendszeren keresztül, mint a PayPal, alacsony értékű tranzakciókkal kapcsolatos terrorizmus finanszírozási ügyeket kapcsoltak össze számos terrorista gyanúsítottal."[74]

***

A 2001. szeptember 11-i terrortámadás után a terrorizmus elleni harc szinte minden országban bekerült az elsődleges preferenciák közé.[75] 2002-ben az Európai Unió kerethatározatában ítélte el a terrorizmust, és kimondta: „Az Európai Unió az emberi méltóság, a szabadság, az egyenlőség és a szolidaritás egyetemes értékei, az emberi jogok és alapvető szabadságjogok tiszteletben tartása alapján áll, s a demokrácia és a jogállamiság – tagállamai által közösen vallott – elvein alapul. A terrorizmus ezen elvek egyik legsúlyosabb megsértése."[76] A magyar Országgyűlés a terrorizmus finanszírozásának visszaszorításáról, New Yorkban, az Egyesült Nemzetek Közgyűlésének 54. ülésszakán, 1999. december 9-én elfogadott nemzetközi egyezményt a 2002. évi LIX. törvénnyel hirdette ki. Ennek az Egyezménynek a 18. cikke kimondja, hogy a „Részes Államok együttműködnek a 2. cikkben meghatározott bűncselekmények megelőzésében minden lehetséges intézkedés megtételével, többek között belső jogszabályaik szükség szerinti, arra irányuló módosításával, hogy területükön

[73] https://elemzeskozpont.hu/szarmaztatott-ugylet-derivativa-jelentese-fogalma-mik-azok.

[74] Serbnakov: i. m. (2022), 98. o.

[75] A terrorizmus elleni hatékony küzdelem csak az integrált bűnüldözés keretében képzelhető el. Ezzel kapcsolatban lásd részletesen Herke Csongor: Integrált bűnüldözés. In Tremmel Flórián – Fenyvesi Csaba – Herke Csongor: *Kriminalisztika.* Budapest, Ludovika Egyetemi Kiadó, 2012, 424–440. o.

[76] A Tanács kerethatározata (2002. június 13.) a terrorizmus elleni küzdelemről, 2002/475/IB, HL 2002 L 164, 2002. június 22., 3.

megelőzzék és elhárítsák az ilyen bűncselekmények területükön vagy területükön kívül történő elkövetését célzó előkészületeket, ideértve [...] azokat az intézkedéseket, amelyek előírják pénzintézeteknek és pénzügyi műveletekkel foglalkozó más hivatást gyakorlóknak, hogy a rendelkezésükre álló leghatékonyabb eljárásokat alkalmazzák szokásos vagy alkalmi ügyfeleik, továbbá azon ügyfeleik azonosítására, akiknek az érdekében számlát nyitnak, továbbá hogy fordítsanak különös figyelmet a szokatlan vagy gyanús műveletekre, és jelentsék be a vélhetően bűnöző tevékenységből származó műveleteket."

A terrorizmus elleni küzdelem anyagi büntetőjogi eszközei a 2001-es amerikai terrortámadások óta mind nemzetközi, mind európai, mind pedig hazai szinten jelentős fejlődésen mentek keresztül. A fellépés összetett jellegét mutatja, hogy nemcsak az egyes tényállások, de az egyéb büntetőjogi intézmények is bekapcsolódtak ezen megújulási folyamatba. Kijelenthető, hogy a terület büntetőjogi leszabályozottsága jelenleg sokkal szélesebb, mint korábban bármikor is volt. A büntetőjogi felelősségre vonás előbbre hozatalát célzó sui generis jellegű tényállások révén lehetőséget ad a büntetőjog arra, hogy már egész „korán" kiemelhetők legyenek a terroristagyanús személyek a társadalomból. Az egységesítő szándék pedig hozzásegít bennünket ahhoz, hogy az egyes terrorizmushoz kapcsolható cselekményeket egyformán lehessen megítélni, azok motivációjától vagy éppen a végrehajtás formájától függetlenül. A terrorizmus elleni küzdelem dimenziónak rendszerében tehát központi helyet kapnak a büntetőjogi eszközök.[77]

A terrorizmus bármely formájáról is legyen szó, a jelenlegi anyagi jogi fegyverzet annak minden, modern kori megnyilvánulásával szemben hatékony eszköz a hatóságok kezében, így büntetőjogi szempontból nem jelent problémát, ha a terrorista akció a kibertér felhasználásával kerül elkövetésre. Minthogy azonban a kifejezetten a kibertérben elkövetett terrorista akciók száma nem mondható kimagaslónak, hiszen a terroristák legfőbb célzata, a félelemkeltés még mindig a klasszikus végrehajtási módokon érhető el a legeredményesebben, figyelmünket alapvetően a terroristák egyéb internethasználati aktivitására kell fordítanunk. Ennek egyrészt az az oka, hogy az egyéb bemutatott célok révén az internet a terrorista szervezetek erősödéséhez, az egyes akciók előkészítéséhez szervesen járulhat hozzá közép- és hosszú távon, másrészt pedig az, hogy ezen internethasználati tevékenység hatóságok általi feltérképezése, lekövetése hozzá tudja segíteni a demokratikus államokat korunk egy legnagyobb biztonsági kihívásával, a nemzetközi terrorizmussal szembeni átfogó fellépés eredményességéhez.

A kiberterrorizmus tehát valós veszély, és ahogyan szokás mondani, „jobb félni, mint megijedni" ezen a fronton, ugyanakkor fontos, hogy a fellépés irányát és

[77] Bartkó Róbert – Farkas Ádám: A terrorizmus elleni harc nemzetközi jog trendjei. In Farkas Ádám – Végh Károly (szerk.): *Új típusú hadviselés a 21. század második évtizedében és azon túl – intézményi és jogi kihívások.* Budapest, Zrínyi Kiadó, 2020, 127. o.

módszertanát jól tudjuk súlypontozni az ellene való küzdelemben. Ebben a tekintetben pedig álláspontom szerint az egyéb internethasználati tevékenységet kell a fókuszpontba helyezni – mivel a klasszikus értelemben vett kiberterrorista akciókkal szembeni fellépés kereteit az anyagi büntetőjog biztosítja –, hiszen ebben a szegmensben lehet a leghatékonyabban megakadályozni a kriminalitás eszkalálódását. A biztonsági kihívás tehát adott, az eszközrendszer pedig folyamatosan fejlődik. Ugyanakkor ez egy olyan próbatétel, ahol a védelmi rendszerek, felderítési módszerek fejlődése is szabadabb környezetben tud megvalósulni. A hangsúly egyértelműen a folyamatos fejlődés igényén van, hiszen maga a kibertér is az állandó változások terrénuma. Ahogyan Nagy fogalmaz már hivatkozott tanulmányában: „a technológiai fejlődés növekedésének üteme exponenciális, azoknak az országoknak, amelyek nem tartanak lépést napjaink fejlődésével, nem alkalmazkodnak a változásokhoz, a lemaradásuk is exponenciális lesz."[78] Az elmúlt időszak védelmi fejlesztései azonban arra engednek következtetni, hogy a demokratikus erők nem kívánnak ilyen mérvű hátrányba kerülni a terrorizmus elleni küzdelemben. Ez pedig mindenképp bizakodásra, biztonságérzetünk erősödésére adhat alapot.

[78] Nagy: i. m. (2018), 38. o.

Bibliográfia

Aar Aaron F. Brantly – Nerea M. Cal – Devlin P. Winkelstein: *Defending the Borderland – Ukrainian Military Experiences with IO, Cyber, and EW.* Army Cyber Institute at West Point, West Point, 2017.

Abishur Prakash: *Go. AI – A mesterséges intelligencia geopolitikája.* Budapest, Pallas Athéné Könyvkiadó, 2018.

Adam Segal: China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace. In Nadége Rolland (szerk.): *An Emerging China-Centric Order – China's Vision for a New World Order in Practice.* Seattle, The National Bureau of Asian Research, 2020.

Alain de Benoist: *Carl Schmitt Today. Terrorism, 'Just' War, and the State of Emergency.* London, Arktos Media Ltd., 2013.

Alexander Klimburg (szerk.): *National Cyber Security Framework Manual.* Tallinn, NATO Cooperative Cyber Defence Centre of Excellence, 2012.

Alix Desforges: *Approche géopolitique du cyberespace, enjeux pour la défense et la sécurité nationale, l'exemple de la France.* Thèse, Université Paris, 2018.

Allison Cavanagh: *Sociology in the Age of the Internet.* Maidenhead, McGrawHill Open University Press, 2007.

Amaël Cattaruzza: *A digitális adatok geopolitikája – A hatalom és konfliktusok a big data korában.* Budapest, Pallas Athéné Könyvkiadó, 2020.

Ambrus István: A 21. századi modernizációra adható büntetőjogi válaszok. *Ügyészek Lapja,* 2019/6. szám., 5-12. o.

Ambrus István: *Digitalizáció és büntetőjog.* Budapest, Wolters Kluwer Hungary Kft., 2021.

Anand – Ch. Raja – E. G. Rajan: Network Centric Warfare- Concepts and Challenges. *CiiT International Journal of Networking and Communication Engineering*, 2011/3. szám..

Andrei Richter: *Regulation of social media in Russia.* Strasbourg, European Audiovisual Observatory, 2021.

Andrew G. McClelland – Roisin Jordan – Szymon Parzniewski –Duncan Shaw – Nat O'Grady – David Powell: Post-COVID Recovery and Renewal through Whole-of-Society Resilience in Cities. *Journal of Safety Science and Resilience*, 2022/3. szám..

Ann Väljataga: *Cyber vigilantism in support of Ukraine: a legal analysis.* Tallinn, CCDCOE, 2022.

Annamária Beláz – Csaba Krasznay – Zsolt Szabó: Cybersecurity Strategy and Leadership Managment Issues. In Živan Živković (szerk.): *An international serial publication for theory and practice of Management Science – IMCSM Proceedings(2020)*, Bor, University of Belgrade, Technical Faculty in Bor, Engineering Management Department (EMD), 2020.

Anthoni Pfaff: The Ethics of Acquiring Disruptive Military Technologies. *Texas National Security Review,* 2019/2020 Winter (https://tnsr.org/2020/01/the-ethics-of-acquiring-disruptive-military-technologies/).

Antonio Missiroli: Geopolitics and strategies in cyberspace: Actors, actions, structures and responses. *Hybrid CoE Paper*, 2021/7. szám..

Árva László – Pásztor Szabolcs – Victoria Pyanatova: A multinacionális vállalati stratégiák és a változó világkereskedelem kapcsolatáról. *Gazdaság és Pénzügy*, 2020/1. szám..

Asa Briggs: The Welfare State in Historical Perspective. In Christopher Piersen – Francis G. Castel (szerk.): *The Welfare State Reader (Second Edition).* Cambridge, Polity Press, 2006.

Asbóth Emma – Tamás Bianka: Szezám tárulj – a kínai szociális kreditrendszer. *Arsboni*, 2019. január 9. (https://arsboni.hu/a-kinai-szocialis-kreditrendszer-sesame-credit/).

Ashley Cha Yin Lim – Pragadesh Natarajan – R. Dineth Fonseka – Monish Maharaj – Ralph J Mobbs: The application of artificial intelligence and custom algorithms with inertial wearable devices for gait analysis and detection of gait-altering pathologies in adults: A scoping review of literature. *Digital Health,* 2022/január (https://journals.sagepub.com/doi/full/10.1177/20552076221074128).

Ashley Collman: Russia disconnected itself from the rest of the internet, a test of its new defense from cyber warfare, report says. *Insider*, 2021. július 23. (https://www.businessinsider.com/russia-cuts-self-off-from-global-internet-tests-defenses-rbc-2021-7).

Atanu Bhuyan: Designing optimal welfare policies for intermediate public transportation systems: A developing country perspective. *Academia Letters (https://www.academia.edu/44905958/Designing_optimal_welfare_policies_for_intermediate_public_transportation_systems_A_developing_country_perspective).*

Aurel Sari: Legal Resilience in an Era of Grey Zone Conflicts and Hybrid Threats. *Exeter Centre for International Law Working Paper* 2019/1. szám..

Bajomi-Lázár Péter – Sükösd Miklós: Médiapolitikai trendek Kelet-Közép-Európában 1989–2008. *Politikatudományi Szemle*, 2009/1. szám..

Bajomi-Lázár Péter: A politika mediatizálódása és a média politizálódása. *Médiakutató*, 2005/ősz.

Balázs István – Hoffman István: A közigazgatási jog rezilienciája – koronavírus idején. In Gárdos-Orosz Fruzsina – Lőrincz Viktor Olivér (szerk.): *Jogi diagnózisok: a COVID-19-világjárvány hatásai a jogrendszerre,* Budapest, L'Harmattan Kiadó – MTA Társadalomtudományi Kutatóközpont, Jogtudományi Intézet, 2020, 45-65. o.

Bándi Gyula: Fenntartható fejlődés, reziliencia és közigazgatás. In Fazekas Marianna (szerk.): *Gazdaság és közigazgatás. Tanulmányok Ficzere Lajos tiszteletére,* Budapest, ELTE Eötvös Kiadó, 2015, 17–26. o.

Bányász Péter – Krasznay Csaba – Tóth András: A NATO kibervédelmi szakpolitikája. In Szenes Zoltán (szerk.): *A mai NATO: A szövetség helyzete és feladatai.* Budapest, HM Zrínyi Térképészeti és Kommunikációs Szolgáltató Nonprofit Kft., 2021.

Bányász Péter – Orbók Ákos: A NATO kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében. *Hadtudomány,* 2013/elektronikus szám

Bányász Péter: *A közösségi média lehetőségei és kihívásai a védelmi szférában.* Doktori (PhD) értekezés. Budapest, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola 2018.

Barabási Albert-László: *Behálózva.* Budapest, Libri Kiadó, 2003.

Baranyi, Péter – Csapó, Ádám – Budai, Tamás – Wersényi, György: Internet of Digital Reality: Infrastructural Background – Part II. *Acta Politechnica Hungarica,* 2021/8. szám..

Baranyi, Péter – Csapó, Ádám – Budai, Tamás – Wersényi, György: Introducing the Concept of Internet of Digital Reality – Part I. *Acta Politechnica Hungarica,* 2021/7. szám..

Barry R. Posen: *Inadvertent Escalation: Conventional War and Nuclear Risks.* Ithaca, Cornell University Press, 1991

Barry Wellmann: The Network Community – An Introduction. In Barry Wellmann (szerk.): *Networks in the Global Village.* New York, Routledge, 2009.

Bartkó Róbert – Farkas Ádám: A terrorizmus elleni harc nemzetközi jog trendjei. In Farkas Ádám – Végh Károly (szerk.): *Új típusú hadviselés a 21. század második évtizedében és azon túl – intézményi és jogi kihívások.* Budapest, Zrínyi Kiadó, 2020.

Bartkó Róbert – Gál István László: A kibertérben megjelenő büntetőjogi kihívások és fenyegetések kezelésének tendenciái, *Military and Intelligence CyberSecurity Research Paper,* 2022/12. szám..

Bartkó Róbert (szerk.): *A terrorizmus elleni küzdelem aktuális kérdései a XXI. században,* Budapest, Gondolat Kiadó, 2019.

Bartkó Róbert: *A terrorizmus elleni küzdelem kriminálpolitikai kérdései.* Győr, UNIVERSITAS-Győr Nonprofit Kft., 2011, 70–79. o.

Bartkó Róbert: *Az irreguláris migráció elleni küzdelem eszközei a hazai büntetőjogban.* Budapest, Gondolat Kiadó, 2020.

Bartkó Róbert: Az Unió 2017/541. sz. Irányelvének hatása a V4 országainak büntető anyagi jogszabályalkotására. In Bartkó Róbert (szerk.): *A terrorizmus elleni küzdelem aktuális kérdései a XXI. században.* Budapest, Gondolat Kiadó, 2019.

Bartóki-Gönczy Balázs – Pogácsás Anett: A médiatartalom-szolgáltatásnak nem minősülő internetes tartalmak szabályozása. In Koltay András – Nyakas Levente (szerk.): *Magyar és európai médiajog.* Budapest, Complex, 2012.

Bartóki-Gönczy Balázs: *Az online közvetítő szolgáltatók mint az információhoz való hozzáférés új kapuőrei.* Budapest, Pázmány Press, 2018.

Bastian Giegreich: Hybrid Warfare and the Changing Character of Conflict. *The Quarterly Journal,* 2016/2. szám..

Beers, R. – Taylors, F. X.: Narco-Terror: The Worldwide Connection Between Drugs and Terror. *Terrorsim and Goverment Information,* 2002.

Ben Buchanan: *The Hacker and the State. Cyber Attacks and the New Normal of Geopolitics.* Cambridge, Harvard University Press, 2020.

Ben Dubow – Edward Lucas – Jake Morris: *Jabbed in the Back: Mapping Russian and Chinese Information Operations During Covid–19.* The Center for European Polidy Analysis (CEPA), 2020.

Béres János (szerk.): *Külföldi nemzetbiztonsági szolgálatok.* Budapest, Zrínyi Kiadó, 2018, 103–107. o.

Béres János: *Napjaink muszlim terrorizmusának gyökerei és visszafordításának lehetőségei.* Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem Hadtudományi Doktori Iskola, doktori értekezés, 2008.

Berki Gábor: *Kiberháborúk, kiberkonfliktusok. Műhelymunkák.* Budapest, Geopolitikai Tanács Közhasznú Alapítvány, 2016.

Bernd Holznagel: Internet freedom, the public sphere and constitutional guarantees. In Monroe E. Price – Stefaan G. Verhulst – Libby Morgan: *Routledge Handbook of Media Law*, London/New York, Routledge, 2013.

Berry, L. V. – Curtis, G. E. – Hudson, R. A. – Kollars, N. A.: *A Global Overview of Narcotics-Funded Terrorist and Other Extremist Groups*, Library of Congress 2002.

Berzsenyi Dániel: Globális kihívás, regionális válaszok: kiberbiztonság Kelet-Közép-Európában. *Nemzet és Biztonság*, 2017/3. szám..

Bihari Mihály: *Politológia – A politika és a modern állam. Pártok és ideológiák.* Budapest, Nemzedékek Tudása Tankönyvkiadó, 2013.

Bognár Zsolt: Az IBM megépítette a világ legnagyobb, 433 qubites kvantumszámítógépét. *Qubit,* 2022. 11. 09. (https://qubit.hu/2022/11/09/az-ibm-megepitette-a-vilag-legnagyobb-433-qubites-kvantumszamitogepet).

Bognár Zsolt: Egy új korszak kezdete: A Google elérte a kvantumfölényt. *Qubit,* 2019. 09. 24. (https://qubit.hu/2019/09/24/egy-uj-korszak-kezdete-a-google-elerte-a-kvantumfolenyt).

Bognár Zsolt: Kína bemutatta a világ legnagyobb teljesítményű kvantumszámítógépét. *Qubit,* 2021. 07. 14. (https://qubit.hu/2021/07/14/kina-bemutatta-a-vilag-legnagyobb-teljesitmenyu-kvantumszamitogepet).

Boris Bucko – Martin Michálek – Katarina Papierniková – Katarína Zábovká: Smart Mobility and Aspects of Vehicle-to-Infrastructure. *Applied Sciences,* 2021/11. szám. (https://www.mdpi.com/2076-3417/11/22/10514/htm).

Boris Toucas: *Understanding the Implications of France's Strategic Review on Defense and National Security.* Center for Strategic and International Studies, 2017.

Bőgel György: *A big data ökoszisztémája.* Budapest, Typotex, 2015.

Böröcz Miklós: Az Európai Unió közös kül-, és biztonságpolitikájának néhány főbb kihívása napjainkban. *Terror & Elhárítás*, 2013/2. szám.

Brandon Valeriano – Benjamin Jensen: *Building a National Cyber Strategy: The Process and Implications of the Cyberspace Solarium Commission Report.* In T. Jancárková – L. Lindström – G. Visky – P. Zotz (szerk.): *13th International Conference on Cyber Conflict: Going Viral.* Tallinn, NATO CCD COE Publications, 2021.

Bruce D. Porter: The Warfare State. *American Heritage*, 1994/4. szám. (https://www.americanheritage.com/warfare-state#1)

Bruce D. Porter: *War and the Rise of the State – The Military Foundations of Modern Politics.* New York, The Free Press, 1994.

Budai Balázs: *Az e-közigazgatás fogalma, jogi és stratégiai keretei.* Budapest, Dialóg Campus, 2017.

Carl Schmitt: A partizán elmélete. In Carl Schmitt: *A politikai fogalma. Válogatott politika- és államelméleti tanulmányok.* Budapest, Osiris – Pallas Stúdió – Attraktor, 2002.

Carl Schmitt: Behemoth, Leviathan und Greif. Vom Wandel der Herrchaftformen. In Carl Schmitt: *Gesammelte Schriften, 1933-1936. Mit ergänzenden Beiträgen aus der Zeit des zweiten Weltkriegs.* Berlin, Duncker & Humblot, 2021.

Carl Schmitt: *Legalitás és legitimitás.* Máriabesnyő–Gödöllő, Attraktor Kft., 2006.

Carol A. Siegel – Mark Sweeney: *Cyber Strategy – Risk-Driven Security and Resiliency.* Boca Raton, CRC Press, 2020.

Caterine Price: *Digitális detox.* Budapest, Libri Könyvkiadó, 2018.

Charles Dunlap Jr.: Lawfare 101 – A Primer. *Military Review*, 2017/May–June, 8–17. o.
Charles E. Lindblom: *A programalkotási folyamat.* Budapest, Budapesti Közgazdaságtudományi Egyetem – Aula Kft., 1995.
Charles J. Dunlap Jr.: *Law and Military Interventions: Preserving Humanitarian Values in 21 st Conflicts.* (https://people.duke.edu/~pfeaver/dunlap.pdf)
Charles Lipson: *Reliable Partners.* Princeton, Princeton University Press, 2003.
Christian Fuchs: *Implications of Deep Packet Inspection (DPI) Internet Surveillance for Society.* Uppsala, Uppsala University, 2012.
Christoper Whyte – Brian Mazanec: *Understanding Cyber Warfare – Politics, Policy and Strategy.* New York, Routledge, 2019.
Christopher Andrew: *Titkos világ I–II.* Budapest, Európa Könyvkiadó, 2021.
Christopher S. Chivvis: *Understanding Russian "Hybrid Warfare" and What Can Be Done About it.* Santa Monica, RAND Corporation, 2017.
Cian C. Murphy: Counter-Terrorism Law and Policy: Operationalisation and Normalisation of Exceptional Law after the 'War on Terror. In Diego Acosta Arcarazo – Cian C. Murphy: *EU Security and Justice Law: After Lisbon and Stockholm.* London, Hart Publishing Ltd., 2014.
Claire Vishik – Mihoko Matsubara – Audrey Plonk: Key Concepts in Cyber Security: Towards a Common Policy and Technology Context for Cyber Security Norms. In Anna-Maria Osula – Henry Roigas (szerk.): *International Cyber Norms: Legal, Policy & Industry Perspectives.* Tallinn, NATO CCD COE Publications, 2016
Concha Győző: *Politika I. Alkotmánytan.* Budapest, Grill Károly Könyvkiadó vállalata, 1907, IX. o.
Corentin Brustlein: Forces Nucléaires Françaises, Quel Renouvellement? *Politique Étrangère*, 2017/3. szám..
Cortney Weinbaum – Bradley Knopp – Kim Soo – Yuliya Shokh: Options for Strengthening All-Source Intelligence. *Rand Corporation Research Report.* 2021 (https://www.rand.org/pubs/research_reports/RRA1245-1.html).
Cortney Weinbaum – Bradley Knopp – Kim Soo – Yuliya Shokh: *Options for Strengthening All-Source Intelligence: Substantive Change Is Within Reach.* RAND Corporation, RR-A1245-1, 2022 (https://www.rand.org/pubs/research_reports/RRA1245-1.html).
Cs. Kiss Lajos: A szociológiai rendszerelmélet államfelfogása. *Jog Állam Politika.* 2010/3. szám..
Cs. Kiss Lajos: A totális állam elmélete és mítosza. *Világosság*, 2010/51. szám. (ősz).
Cs. Kiss Lajos: Alkotmányelmélet és az érték logikája: zsarnokság vagy szabadság? *Jog Állam Politika*, 2017/3. szám..
Csiki Tamás – Tálas Péter – Varga Gergely: A NATO walesi csúcstalálkozójának napirendje és értékelése. *Nemzet és Biztonság*, 2014/4. szám..
Csitei Béla: Az önvezető járművek és az Európai Unió joga. In Lévayné Fazekas Judit – Kecskés Gábor (szerk.): *Az autonóm járművek és intelligens rendszerek jogi vonatkozásai.* Győr, Universitas–Győr Nonprofit Kft., 2020.
Csizmadia Norbert: *Geopillanat. A 21. század megismerésének térképe.* Budapest, L'Harmattan, 2016.
Damien Van Puyvelde – Aaron F. Brantly: *Cybersecurity – Politics, Governance and Conflict in Cyberspace.* Cambridge, Polity Press, 2019.

Daniel Mack: An Era of Foreign Political Interference: Impulsive, Overcompensation of Australia, and a Comparison of Legislative Schemes with the United States. *Emory International Law Review*, 2020/1. szám..

Danyiil Turovszkij: *Orosz hekkerek. Így lettek lázadókból Putyin katonái.* Budapest, Athenaeum, 2020.

David A Graham: Cyber Threats and the Law of War. *Journal of National Security Law & Policy*, 2010/1. szám..

David Carment – Dani Belo: *War's Future: The Risks and Rewards of Grey Zone Conflict and Hybrid Warfare.* Calgary, Canadian Global Affairs Institiute, 2018.

David Edgerton: *Warfare State – Britain, 1920–1970.* Cambridge, Cambridge University Press, 2006.

David Epstein: *Sokoldalúság.* Budapest, HVG Könyvek Kiadó, 2021.

David Wallace: Cyber Weapon Reviews under International Humanitarian Law: *A Critical Analysis. Tallinn Paper No 11.* Tallinn, NATO Cooperative Cyber Defence Centre of Excellence, 2018.

Debashis Majumdar – Pradipta Kumar Banerji – Satyajit Chakrabarti: Disruptive technology and disruptive innovation: ignore at your peril!: *Technology Analysis & Strategic Managment,* 2018/11. szám..

Deborah Lupton: Digital *Sociology.* London – New York, Routledge, 2015.

Desewffy Tibor: *Digitális szociológia.* Budapest, Typotex Kiadó, 2019.

Dobák Imre: Nemzetbiztonsági szolgálatok - Betekintés a visegrádi országok (V4) nemzetbiztonsági rendszereibe. *Hadtudomány,* 2015/4. szám., 114. o.

Dornfeld László: Kiberterrorizmus – a jövő terrorizmusa? In Mezei Kitti (szerk.): *A bűnügyi tudományok és az informatika.* Pécs, Budapest, PTE ÁJK – MTA Társadalomtudományi Kutatóközpont, 2019.

Douglas Murray: *A tömegek tébolya – Áldozatok a politikai korrektség oltárán?* Budapest, Alexandra, 2020.

Dragoş-Mihai Păunescu: NATO's encounters in the cyber domain. *Proceedings of the 17th International Scientific Conference „Strategies XXI" – Strategic Changes in Security and International Relations*, 2021/1. szám..

Dusek Tamás: Az okos városok komplex mutatószámainak egyes tartalmi és módszertani problémái. In Kovács Gábor – Völgyi Katalin (szerk.): *Üzleti vállalkozások, makro- és mikrokörnyezetük gazdálkodási és menedzsment sajátosságai c. kutatás tanulmányai.* Győr, Széchenyi István Egyetem Kautz Gyula Gazdaságtudományi Kar, 2018.

Eck Gábor: Az online terrorista tartalmak elleni fellépést támogató uniós és magyarországi intézkedések. *Külügyi Műhely,* 2022/4. szám., 34–48. o.

Edvi Illés Károly: *Az anyagi büntető törvények és a sajtótörvény.* Budapest, Grill Károly Könyvkiadó Vállalata, 1907.

Edward D. Mansfield: Concentration, Polarity, and the Distribution of Power. *International Studies Quarterly,* 1993/1. szám..

Edward Geist – Andrew J. Lohn: *How Might Artificial Intelligence Affect the Risk of Nuclear War?* Santa Monica, CA: RAND Corporation, 2018; Kareem Ayoub – Kenneth Payne: Strategy in the Age of Artificial Intelligence. *Journal of Strategic Studies,* 2016/5–6. szám..

Engel Péter: A Bundeskartellamt Facebook-döntése – az adatgyűjtés versenyjogi kockázatai. *Verseny Tükör,* 2019/1. szám..

Eric Gartzke – Li Quan Li – Charles Boehmer: Investing in the Peace. *International Organization*, 2001/Spring.

Eric Weede: Democracy and War Involvement. *Journal of Conflict Resolution*, 1984/4. szám..

Erik Reichborn-Kjennerud – Patrick Cullen: What is Hybrid Warfare? *Policy Brief,* 2016/1. szám..

Ernst Jünger: *Waldgang*. Stuttgart, Klett-Cotta, 1980; Békés Márton: Erdei séta (Waldgang-kommentár). In Békés Márton: *Az utolsó felkelés*. Budapest, Századvég Kiadó, 2014.

Farkas Ádám – Resperger István: Az úgynevezett „hibrid hadviselés" kihívásainak kezelése és a nemzetközi jog mai korlátai. In Farkas Ádám – Végh Károly (szerk.): *Új típusú hadviselés a 21. század második évtizedében és azon túl. Intézményi és jogi kihívások.* Budapest, Zrínyi Kiadó, 2020.

Farkas Ádám – Spitzer Jenő: Az információs korszak és az állami reziliencia egyes kérdései. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok*, 2021/18. szám.

Farkas Ádám (szerk.): *Védelmi alkotmányosság az új típusú biztonsági kihívások erőterében.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2018.

Farkas Ádám: *A fegyveres védelem mint állami alrendszer és annak szabályozási sajátosságai.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2018.

Farkas Ádám: A katonai büntetőjog és igazságszolgáltatás helye, szerepe, létjogosultsága az állam és társadalom rendszereiben. *Hadtudomány*, 2012/elektronikus szám.

Farkas Ádám: A kibertérműveleti képességek kialakításának és fejlesztésének egyes szabályozási és államszervezési alapvonalai. *Jog Állam Politika*, 2019/2. szám..

Farkas Ádám: A kortárs technológia-fejlődés és innováció viszonya a honvédelmi szabályozással. *MTA Law Working Paper,* 2021/4. szám..

Farkas Ádám: A multidiszciplinaritás helye, szerepe a védelem és biztonság szabályozásának és szervezésének komplex kutatásaiban. *Közjogi Szemle,* 2021/4. szám..

Farkas Ádám: A terrorizmus elleni harc, mint kiemelt ágazatközi fegyveres védelmi feladat. *Szakmai Szemle*, 2017/3. szám..

Farkas Ádám: A totális államtól a totális háborún át a totális védelemig. *MTA Law Working Papers*, 2015/34. szám..

Farkas Ádám: *A totálitás kora? A 21. század biztonsági környezetének és kihívásainak totalitása és a totális védelem gondolatkísérlete.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2018.

Farkas Ádám: A történelmi tapasztalat és a tudomány helye, szerepe a 21. századi védelmi és biztonsági gondolkodásban. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok* 2022/1. szám..

Farkas Ádám: *A védelem és biztonság-szavatolás szabályozásának alapkérdései Magyarországon.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2022.

Farkas Ádám: A védelmi-biztonsági gondolkodás és képzés megújításának elméleti és kulturális alapjai. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok*, 2022/2. szám..

Farkas Ádám: *Az állam fegyveres védelmének alapvonalai.* Budapest, Katonai Nemzetbiztonsági Szolgálat, 2020.

Farkas Ádám: Az állam védelmi kötelezettségeinek egyes kortárs aspektusai. *Jogelméleti Szemle*, 2018/4. szám..

Farkas Ádám: Biztonság – Geopolitika – Digitalizáció, avagy Amaël Cattaruzza „A digitális adatok geopolitikája" című kötetének főbb üzenetei. *SmartLaw Research Group Working Paper*, 2021/1. szám..

Farkas Ádám: Gondolatok a 21. századi biztonságról, államról, védelemről. *Hadtudomány*, 2018/elektronikus szám.

Farkas Ádám: Gondolatok a nemzetbiztonság fogalmáról. In Szakmai Szemle 2020/3. szám., 5–20. o.

Farkas Ádám: Gondolatok a terrorveszélyhelyzetről. *Szakmai Szemle*, 2016/3. szám..

Farkas Ádám: Gondolatok a totalitás 21. századi esszenciájához. In Pongrácz Alex (szerk.): *Ünnepi tanulmányok a 65 éves Cs. Kiss Lajos tiszteletére. Út vocatio scientia.* Budapest, Ludovika Egyetemi Kiadó, 2021.

Farkas Ádám: Kibertér művelet: hírszerző, rendészeti és katonai műveletek elegye? Gondolatok az angol National Cyber Force kapcsán. *Military and Intelligence CyberSecurity Research Paper*, 2021/1. szám..

Farkas Ádám: Szemléletváltást védelmi aspektusban! *Pázmány Law Working Papers*, 2015/18. szám..

Farkas Ádám: The UK'S National Cyber Force – Beginning of a Hybrid Trend or a New Answer for Cyber Domain. In *Military and Intelligence CyberSecurity Research Paper,* 2022/2.

Fekete Csanád: Információ és hadviselés háború a kognitív hadszíntéren II. *Szakmai Szemle*, 2016/4. szám..

Fekete Csanád: Információ és hadviselés háború a kognitív hadszíntéren II. *Szakmai Szemle*, 2016/3. szám..

Fekete-Karydis Klára – Lázár Bence: A kibervédelem katonai dimenziói. *Hadtudományi Szemle*, 2020/3. szám..

Ferdinandy László: Államalakulatok és államalkotó eszmék. Történelembölcseleti tanulmányok III. *Magyar Kultura* [*Kultúra*], 1924/10. szám..

Ferencz Jácint: Az információ és a technológia kettős arca a munkajogban. In Baranyiné Kóczy Judit – Fehér Ágota (szerk.): *Pedagógusképzés, oktatás a Kárpát-medencében, társadalmi kontextusok. XXII. Apáczai-napok Tudományos Konferencia tanulmánykötet.* Győr, Széchenyi István Egyetem Apáczai Csere János Kar, 2019.

Forgács Imre: *Az eltűnő munka nyomában. A Big Data és a pénztőke évszázada.* Budapest, Gondolat Kiadó, 2015, különösen.

Forrest E. Morgan et al.: *Dangerous Thresholds: Managing Escalation in the 21st Century.* Santa Monica, CA: RAND Corporation, 2008.

Francis Fukuyama: *Identity – The Demand for Dignity and the Politics of Resentment.* Farrar, Straus and Giroux, New York, 2018.

Frank G. Hoffman: Hybrid Warfare and Challenges. *Joint Force Quarterly,* 2009/1st quarter.

Fred J. Cook: The Warfare State. *The Annals of the American Academy of Political and Social Scince*, 1964/1. szám..

Frédérick Douzet: Geopolitika a kibertér megértéséhez. In Dornfeld László – Keleti Arthur – Barsy Miklós – Kilin Józsefné – Berki Gábor – Pintér István: *A virtuális tér geopolitikája. Tanulmánykötet.* Budapest, Geopolitikai Tanács Közhasznú Alapítvány, 2016.

Gál István László: *A terrorizmus finanszírozása. Die Terrorismusfinanzierung,* Pécs, Pécsi Tudományegyetem Állam- és Jogtudományi Kar Gazdasági Büntetőjogi Kutatóintézet Pécs, 2010.

Gárdos-Orosz Fruzsina: Az alapjogok korlátozása. In Jakab András – Könczöl Miklós – Menyhárd Attila – Sulyok Gábor (szerk.): *Internetes Jogtudományi Enciklopédia*; 2020.
Gazdag Erika: Koncepciófejlesztés a NATO-ban. *Honvédségi Szemle*, 2022/3. szám..
Gellén Klára: Tisztességtelen kereskedelmi gyakorlatok az online térben – fókuszban a közösségi média. *In Medias Res*, 2020/1. szám..
Gémes Csaba: A kibertér és szereplői. *Hadmérnök,* 2018/3. szám..
Georg Jellinek: *Általános államtan.* Budapest, ELTE ÁJK TEMPUS Összehasonlító Jogi Kultúrák, 1994.
Georg Nolte: *European Military Law Systems.* Berlin, De Gruyter Rect, 2003.
Gergely Attila: A terrorizmus természetrajza. *Kapu*, 1994/10–11. szám..
Gerhard Wisnewski – Wolfgang Landgraeber – Ekkehard Sieker: *Das RAF-Phantom Neue Ermittlungen in Sachen Terror.* München, Knaur Taschenbuch Verlag, 2008.
Gerry Mackie: Reviewed. *Notre Dame Philosophical Reviews*, 2007. (http://ndpr.nd.edu/news/23149/?id=11143)
Gordon E. Moore: Cramming more components onto integrated circuits. *Electronics,* 1965/8. szám..
Gøsta Esping-Andersen: A Welfare State for the Twenty–first Century. In Christopher Piersen – Francis G. Castel (szerk.): *The Welfare State Reader (Second Edition).* Cambridge, Polity Press, 2006.
Gøsta Esping–Andersen: Towards the Good Society, Once Again? In Gøsta Esping-Andersen (szerk.): *Why We Need a New Welfare State.* Oxford – New York, Oxford University Press, 2002.
Gosztonyi Gergely: A kínai internetcenzúra modellje. *Pro Futuro,* 2022/1. szám..
Gosztonyi Gergely: Az internetes tartalomszabályozással kapcsolatos új gondolkodási irányok az Amerikai Egyesült Államokban. *Miskolci Jogi Szemle*, 2021/4. szám..
Gosztonyi Gergely: Az internet-hozzáférés korlátozásának gyakorlata az Emberi Jogok Európai Bírósága előtt. *In Medias Res,* 2021/1. szám..
Gosztonyi Gergely: *Cenzúra Arisztotelésztől a Facebookig – A közösségi média tartalomszabályozási gyakorlatának komplexitása.* Budapest, Gondolat Kiadó, 2022.
Gosztonyi Gergely: Special Models of Internet and Content Regulation on China and Russia. *ELTE Law Journal*, 2021/2. szám..
Gosztonyi, Gergely: The European Court of Human Rights: Internet access as a means of receiving and imparting information and ideas. *International Comparative Jurisprudence Research Journal,* 2020/2. szám..
Gregory F. Treverton – Andrew Thyedt – Alicia R. Chen– Kathy Lee – Madeline McCue: *Adressing Hybrid Threats.* Stockholm, Swedish Defence University, 2018.
Gregory Falco – Eric Rosenbach: *Confronting Cyber Risk – An Embedded Ensurance for Cybersecurity.* Oxford, Oxford University Press, 2022.
Gregory M. Kaladijan: Welfare vs Cyberfare. *Journal of Children and Proverty*, 1996/1. szám..
Guido Pincione – Fernando Tesón: *Rational Choice and Democratic Deliberation: A Theory of Discourse Failure.* Cambridge University Press, 2006.
Gunaratna R: *Inside Al Quaeda: Global Network of Terror.* London, Hurst&Company, 2002.
Gyekiczky Tamás: *Olvasmányok a Digitális társadalomról – jogászoknak* (kézirat). Budapest, 2021 (https://www.academia.edu/49694295/Olvasm%C3%A1nyok_a_Digit%C3%A1lis_T%C3%A1rsadalomr%C3%B3l_Jog%C3%A1szoknak).

Győrfi Tamás: 2. § [Alkotmányos alapelvek; ellenállási jog.] In Jakab András (szerk.): *Az Alkotmány kommentárja.* Budapest, Századvég, 2009.

Haig Zsolt – Kovács László: Fenyegetések a cybertérből. *Nemzet és Biztonság*, 2008/5. szám..

Haim Assa: *Cyberspace and its effect on cultural-political and social processes.* Tel Aviv, Tel Aviv University, 2011.

Hajdú József: A mesterséges intelligencia hatása a munkaerőpiacra, avagy elveszik-e a robotok az ember munkáját. *Infokommunikáció és Jog,* 2020/2. szám..

Hajdu Péter: A kibertér etikai, jogi és társadalmi kihívásai. *Új Pedagógiai Szemle,* 2001/7–8. szám..

Hamid Jahankhani – Liam M. O'Dell – Gordon Bowen – Danial Hagan – Arshad Jamal: *Strategy, Leadership, and AI in the Cyber Ecosystem – The role of digital societies in infromation governance and decision making.* London, Academic Press, 2021.

Hans M. Kristensen – Matthew McKinzie – Theodore A. Postol: How US Nuclear Force Modernization Is Undermining Strategic Stability: The Burst-Height Compensating Super-Fuze. *Bulletin of the Atomic Scientists*, 2017 (https://thebulletin.org/2017/03/how-us-nuclear-force-modernization-is-undermining-strategic-stability-the-burst-height-compensating-super-fuze/).

Harkai István: Végfelhasználói jogok a digitális szerzői jogban: Felhasználói jogok…? In Strihó Krisztina – Szegedi László (szerk.): *Európai szabályozáspolitikai kihívások.* Budapest, Ludovika Egyetemi Kiadó, 2022, 25–31. o.

Helena Carrapico – Andre Barrinha: European Union cyber security as an emerging research and policy field. *European Politics and Society,* 2018/3. szám..

Hendlein Teréz – Prazsák Gergő: A hálózati társadalom receptje. *Információs Társadalom,* 2005/4. szám..

Herke Csongor: Integrált bűnüldözés. Tremmel Flórián –Fenyvesi Csaba – Herke Csongor: *Kriminalisztika.* Budapest, Ludovika Egyetemi Kiadó, 2012.

Hódos László: A hibrid konfliktusok felívelési szakasza, avagy a fenyegetés észlelésének, megelőzésének és kezelésének nemzetbiztonsági aspektusai. *Honvédségi Szemle*, 2020/4. szám..

Hódos László: A hibrid konfliktusok felívelési szakasza, avagy a fenyegetés észlelésének, megelőzésének és kezelésének nemzetbiztonsági aspektusai. *Honvédségi Szemle*, 2020/4. szám., 49–64. o.

Hódos László: Gondolatok a nemzeti hírszerző képesség koordinációjáért felelős szerv közjogi helyzetéről. *Szakmai Szemle*, 2018/4. szám..

Hódos László: Gondolatok a nemzeti hírszerző képesség koordinációjáért felelős szerv közjogi helyzetéről, *Szakmai Szemle,* 2018/4. szám., 5–16. o.

Hoffman István – Kádár Pál: A különleges jogrend és a válságkezelés közigazgatási jogi kihívásai. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* 2021/2. szám..

Horváth Barna: *Angol jogelmélet.* Budapest, A Magyar Tudományos Akadémia Kiadása, 1943.

Incze Norbert – Pesuth Tamás: E-Health – Digitalizálódik az egészségügy? *Köz-Gazdaság,* 2020/4. szám..

Irene Connolly – Marion Palmer – Hannah Barton – Gráinne Kirwan (ed.): *An Introduction to Cyberpsychology.* London – New York, Routledge, 2016.

J. R. Koza – F. H. Bennett – D. Andre – M. A. Keane: Automated Design of Both the Topology and Sizing of Analog Electrical Circuits Using Genetic Programming. In J. S. Gero – F. Sudweeks (szerk.): *Artificial Intelligence in Design.* Dordrecht, Springer, 1996.

James Fearon: Domestic Political Audiences and the Escalation of Political Disputes. *American Political Science Review*, 1994/3. szám..

James G. March: *Bevezetés a döntéshozatalba.* Budapest, Panem Könyvkiadó, 2000.

James S. Johnson: Artificial Intelligence and Future Warfare: Implications for International Security. *Defense and Security Analysis,* 2019/2. szám..

James S. Johnson: Artificial Intelligence: A Threat to Strategic Stability. *Strategic Studies Quarterly*, 2020/1. szám..

James T. Sparrow: *Warfare State – World War II Americans and the Age of Big Government.* Oxford, Oxford University Press, 2011.

Jarmo Makela: Countering Disinformation: News Media and Legal Resilience. *Hybrid CoE Paper,* 2019/1. szám..

Jessica Davis: *New Technologies but Old Methods in Terrorism Financing.* London, Royal United Services Institute for Defence and Security Studies, 2020.

Jessika Aro: *Putyin trolljai – Igaz történetek az orosz infoháború frontvonalából.* Budapest, Corvina, 2021.

Jessilyn Dunn – Lukasz Kidzinski – Ryan Runge et al.: Wearable sensors enable personalized predictions of clinical laboratory measurements. *Nature medicine,* 2021, 27. kötet (https://nmbl.stanford.edu/wp-content/uploads/Dunn-Nature-Med-2021.pdf).

Joan Barata: The different concepts of free expression and its link with democracy, the public sphere and other concepts. In Monroe E. Price – Stefaan G. Verhulst – Libby Morgan (szerk.): *Routledge Handbook of Media Law.* London/New York, Routledge, 2013.

Johm Campbell: Nigerian President Buhari Clashes With Twitter Chief Executive Dorsey. *Council on Foreign Relations Blog*, 2021. július 8. (https://www.cfr.org/blog/nigerian-president-buhari-clashes-twitter-chief-executive-dorsey).

John Carlson – Neville Yeomans: Whither Goeth the Law – Humanity or Barbarity, a The Way Out – Radical Alternatives in Australia. In M. Smith – D. Crossley (szerk.): *Lansdowne.* Melbourne, 1975 (http://www.laceweb.org.au/whi.htm).

John Graham – Bruce Amos – Tim Plumptre: *Principles for Good Governance in the 21st Century.* Ottawa, Institute on Governance – Policy Brief No. 15., 2003.

John Mearsheimer: Back to the Future. *International Security,* 1990/1. szám..

John Mueller: *Retreat from Doomsday.* New York, Basic Books. 1989.

John P. Carlin: Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats. *Harvard Law School National Security Journal*, 2016.

John R. Suler: *Psychology of the Digital Age: Humans Become Electric.* Cambridge, Cambridge University Press, 2015.

John W. Tammen: NATO's Warfighting Capstone Concept: anticipating the changing character of war. *NATO Review.* 2021 (https://www.nato.int/docu/review/articles/2021/07/09/natos-warfighting-capstone-concept-anticipating-the-changing-character-of-war/index.html).

Jones Craig A.: Lawfare and the Juridification of Late Modern War. *Progress in Human Geography* 2016/2. szám..

Juhász István – Petruska Ferenc: A védelmi-biztonsági szabályozási reformot indukáló biztonsági környezet-változás elemeinek beazonosítása, szakmai értéeklése. *Védelmi-biztonsági Szabályozási és Kormányzástani Kutatóműhely,* 2022/32. szám..

Jürgen Altmann – Frank Sauer: Autonomous Weapon Systems and Strategic Stability. *Survival,* 2017/5. szám..

Jürgen Habermas: *A társadalmi nyilvánosság szerkezetváltozása.* Budapest, Osiris, 1999.

K. Seethal – B. Menaka: Digitalisation Of Education In 21ST Century: A Boon Or Bane. *International Journal for Research in Engineering Application & Management,* 2019 (http://www.ijream.org/SpecialIssueConference/ICDOMP2019036.pdf).

Kádár Pál: A védelmi-biztonsági szabályozás reformjának egyes kérdései az Alaptörvényen túl. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* 2021/11. szám..

Kaiser Tamás – Bozsó Gábor: Az államközpontú kormányzás koncepciójának és mérhetőségének főbb aspektusai. *Államtudományi Műhelytanulmányok*, 2016/22. szám..

Kaiser Tamás – Kis Norbert (szerk.): *A jó állam mérhetősége.* Budapest, Nemzeti Közszolgálati Egyetem, 2014.

Kaiser Tamás (szerk.): *A jó állam nagyító alatt: speciális jelentések A-tól V-ig (az adóbürokráciától a versenyképességig).* Budapest, Dialóg Campus Kiadó, 2016.

Kálmán Kinga: Nyomokban kódokat tartalmazhat? A mesterséges intelligencia igazságszolgáltatásban történő alkalmazásának alkotmányjogi vonatkozásai a tisztességes eljáráshoz való jog tükrében. *MTA Law Working Papers,* 2021/2. szám..

Karácsony Gergely: A videójátékok adatkezelési gyakorlata: kommunikáció és profilalkotás. In G. Karácsony Gergely (szerk.): *A videojátékok jogi kérdései.* Győr, Széchenyi István Egyetem, 2021.

Karácsony Gergely: *Okoseszközök – okos jog?* Budapest, Ludovika Egyetemi Kiadó, 2020.

Kassai Károly: Az elektronikus információvédelem felső szintű szervezeti és szakmai történései a 2005–2015 közötti időszakban. *Hadmérnök*, 2015/3. szám..

Kate Jean Dent: Lawfare and Legitimacy: *The Wicked Problem of Judicial Resilience at a Time of Judicialisation of Politics in South Africa (doctoral dissertation).* Cape Town, University of Cape Town, Faculty of Law, 2021 (https://open.uct.ac.za/handle/11427/35641).

Katharina Ziolkowski: Peacetime Cyber Espionage – New Tendenciesin Public International Law. In Katharina Ziolkowski (szerk.): *Peacetime Regime for State Activitiesin Cyberspace International Law, International Relations and Diplomacy.* Tallinn, NATO Cooperative Cyber Defence Centre of Excellence Publication, 2013.

Kecskés András – Halász Vendel – Bujtár Zsolt: *Tőzsdeuniverzum.* Budapest, HVG-ORAC Kiadó, 2019.

Kecskés Gábor: Az autonóm járművek jogi kérdéseinek nemzetközi kontextusa, különös tekintettel a környezetjogi vetületekre. *Állam- és Jogtudomány,* 2020/4. szám..

Keith L. Nelson: The Warfare State: History of Concept. *Pacific Historical Review,* 1971/2. szám.

Kelemen, Roland – Farkas, Ádám: To the Margin of the Theory of a New Type of Warfare: Examining Certain Aspects of Cyber Warfare. In Szabó, Marcel – Gyeney, Laura – Láncos, Petra Lea (szerk.): *Hungarian Yearbook of International law and European Law (2019).* Den Haag, Eleven International Publishing, 2020

Kelemen Roland – Mihály Laura Dominika: A kibertér és a psziché ütközéspontjai mint a 21. századi reziliencia kulcskérdése. *Védelmi-biztonsági Szabályozási és Kormányzástani Kutatóműhely*, 2022/14. szám..

Kelemen Roland – Németh Richárd: A kibertér alanyai és sebezhetősége. *Szakmai Szemle*, 2019/3. szám..

Kelemen Roland – Németh Richárd: A kibertér fogalmának és jellemzőinek multidiszciplináris megközelítése. In Farkas Ádám (szerk.): *Védelmi alkotmányosság az új típusú biztonsági kihívások erőterében.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2018.

Kelemen Roland – Németh Richárd: Társadalmi hálózatok és reziliencia. *Védelmi-biztonsági Szabályozási és Kormányzástani Kutatóműhely*, 2022/13. szám..

Kelemen Roland – Pataki Márta: A kibertámadások nemzetközi jogi értékelése. *Katonai Jogi és Hadijogi Szemle*, 2015/1. szám..

Kelemen Roland – Pataki Márta: Kiberterrorizmus: A terrorizmus új arca. *Magyar Rendészet*, 2014/5. szám..

Kelemen Roland – Simon László: A kibertérben megjelenő fenyegetések és kihívások kezelésének egyes nemzetközi jogi problémái. In Farkas Ádám – Végh Károly (szerk.): *Új típusú hadviselés a 21. század második évtizedében és azon túl– intézményi és jogi kihívások.* Budapest, Zrínyi Kiadó, 2020.

Kelemen Roland: A derogáció értelmezése a Polgári Jogok Nemzetközi Egyezségokmányának, valamint az Emberi Jogok Európai Egyezményének tükrében. *Közjogi Szemle*, 2018/4. szám..

Kelemen Roland: A kibertérből érkező fenyegetések jelentősége a hibrid konfliktusokban és azok várható fejlődése. *Honvédségi Szemle*, 2020/4. szám..

Kelemen Roland: A nem állami kibertéri műveletek egyes szereplőinek jelentősége a hibrid konfliktusokban. *Smart Law Research Group Working Paper*, 2021/2. szám..

Kelemen Roland: A polgári kor társadalombiztosítása – Társadalombiztosítási bíráskodás a polgári korban. In Molnár Andrea – Széplaki László (szerk.): *Tanulmányok a győri felsőbíráskodás történetéből a XIX–XX. század fordulóján.* Győr, Győri Ítélőtábla, 2019.

Kelemen, Roland: Cyber Attacks and Cyber Intelligence in the System of Cyber Warfare. In Szabó Miklós (szerk.): *Doktoranduszok Fóruma Miskolc 2016. november 17. Állam- és Jogtudományi Kar szekciókiadványa.* Miskolc, Miskolci Egyetem, 2017

Kelemen Roland: Cyberfare state – Egy hibrid állammodell 21. századi születése. *Military and Intelligence CyberSecurity Research Paper,* 2022/1. szám..

Kelemen Roland: Pillanatképek a kivételes állapot elméleti kérdéseinek köréből. *Katonai Jogi és Hadijogi Szemle*, 2016/1–2. szám..

Kelemen Roland: Radikalizálás, dezinformálás és tömegpszichózis modern köntösben: a hibrid konfliktus kibertérben. *Jog Állam Politika,* 2021/3. szám..

Kenedli Tamás – Kis-Benedek József – Szabó Károly: A katonai felderítés és elhárítás evolúciója, szervezete és feladatkörei. In Farkas Ádám – Kádár Pál (szerk.): *Magyarország katonai védelmének közjogi alapjai.* Budapest, HM Zrínyi Térképészeti és Kommunikációs Szolgáltató Közhasznú Nonprofit Kft., 2016.

Kenedli Tamás: A Katonai Nemzetbiztonsági Szolgálat szakmai fejlődésének legfontosabb sajátosságai az elmúlt években. *Nemzetbiztonsági Szemle*, 2020/1. szám..

Kenneth Geers (szerk.): *Cyber War in Perspective: Russian Aggression against Ukraine.* Tallinn, NATO Cooperative Cyber Defence Centre of Excellence, 2015.

Kenneth Schultz: Domestic Opposition and Signaling in International Crises. *American Political Science Review*, 1998/4. szám..

Keserű Barna Arnold: A mesterséges intelligencia néhány magánjogi aspektusáról. In Glavanits Judit (szerk.): *A gazdasági jogalkotás aktuális kérdései.* Budapest, Dialóg Campus, 2019.

Keszely László: A hibrid konfliktusokkal szembeni átfogó fellépés lehetséges kormányzati modelljei. *Honvédelmi Szemle*, 2020/4. szám..

Keszely László: *A védelmi igazgatás szerepe a nemzeti szintű átfogó megközelítés megvalósításában.* Budapest, Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, doktori értekezés, 2017.

Keszely László: Hibrid hadviselés és nemzeti ellenálló képesség (resilience), avagy átfogó megközelítés újratöltve. *Katonai Jogi és Hadijogi Szemle*, 2018/1. szám..

Kieron O'Hara – Wendy Hall: Four Unternets. The Geopolitics of Digital Governance. *CIGI Papesrs No. 206.* Waterloo, Centre for International Governance Innovation, 2018.

Kiss Álmos Péter: A hibrid hadviselés természetrajza. *Honvédségi Szemle*, 2019/4. szám..

Kiss Attila – Krasznay Csaba: A felhasználói viselkedéselemzés kiberbiztonsági előnyei és adatvédelmi kihívásai. *Információs Társadalom: Társadalomtudományi Folyóirat*, 2017/1. szám..

Kiss Tibor – Parti Katalin – Prazsák Gergő: *Cyberdecinacia.* Budapest, Dialóg Campus, 2019.

Kiss Tibor: *Agresszió a cybertérben.* Budapest, Nemzeti Közszolgálati Egyetem, 2020; Kiss Tibor – Pari Katalin – Prazsák Gergő: *Cyberdeviancia.* Budapest, Dialóg Campus, 2019.

Kittrie Orde: *Lawfare: law as a weapon of war.* Oxford, New York, Oxford University Press, 2016.

Klein Tamás – Tóth András: A robotika egyes szabályozási kérdései. In Homicskó Árpád Olivér (szerk.): *Egyes modern technológiák etikai, jogi és szabályozási kihívásai.* Budapest, Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, 2018.

Kollár Csaba: Kína és a társadalmi kredit rendszere. *Hadtudomány,* 2020/2. szám..

Koltay András: A médiaszabályozás elmélete. In Koltay András – Nyakas Levente (szerk.): *Magyar és európai médiajog.* Budapest, Complex, 2012.

Koltay András: A social media platformok jogi státusa a szólásszabadság nézőpontjából. *In Media Res,* 2019/1. szám..

Koltay András: Az internetes kapuőrök és az Emberi Jogok Európai Egyezményének 10. cikke – a sajtószabadság új alanyai. *Állam- és Jogtudomány*, 2017/4. szám..

Korinek László: A terrorizmus. Gönczöl Katalin – Kerezsi Klára – Korinek László – Lévay Miklós (szerk.): *Kriminológia-Szakkriminológia.* Budapest, CompLex Kiadó, 2006.

Korinek László: *Kriminológia.* Budapest, Magyar Közlöny Lap- és Könyvkiadó Kft., 2010.

Kovács József: A Katonai Nemzetbiztonsági Szolgálat az egyesítés után. *Hadtudomány,* 2013/1–2. szám..

Kovács László – Krasznay Csaba: „Mert övék a hatalom": Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során. *Nemzet és Biztonság*, 2017/3. szám..

Kovács László: *A kibertér védelme.* Budapest, Dialóg Campus, 2018.

Kovács László: Cyber Security Policy and Strategy in the European Union and NATO. *Land Forces Academy Review*, 2018/1. szám..

Kovács László: *Kiberbiztonság és -stratégia.* Budapest, Dialóg Campus, 2018.

Kovács Zoltán – Gurály Roland: A mesterséges intelligencia és egyéb felforgató technológiák hatásainak vizsgálata. *Felderítő Szemle*, 2021/2. szám..

Kovács-Szépvölgyi Enikő (szerk.): *Kihívások a büntetőjogi jogalkotás terrénumában a 19–21. században. Külföldi minták és nemzeti megoldások.* Budapest, Gondolat Kiadó, 2022.

Kun István – Fáy Gyula – Bukovics István: Logikai hadviselés – Kritikus pontok harca. *Hadmérnök.* 2011/ 4. szám..

Kun Zsuzsi: A világ legnagyobb 3,2 gigapixeles digitális kamerája magasabb egy autónál, és galaxisok milliárdjait örökítheti meg. *Qubit,* 2022. 10. 28. (https://qubit.hu/2022/10/28/a-vilag-legnagyobb-32-gigapixeles-digitalis-kameraja-magasabb-egy-autonal-es-galaxisok-milliardjait-orokitheti-meg).

Kurt Gaubatz: Democratic States and Commitment in Inter national Politics. *International Organization*, 1996/1. szám..

Kyle Mizokami: Anti-Satellite Weapons Are Becoming a Very Real Threat. *Popular Mechanics.* 2020 (https://www.popularmechanics.com/military/weapons/a32008306/anti-satellite-weapons/).

L. Samuel: Some studies in machine learning using the game of checkers. *IBM Journal of Research and Development*, 1959/3. szám..

Lajtár István: A kiberbűnözésről. *Ügyészek Lapja,* 2019/1. szám..

Lapsánszky András: A COVID-19 járvány hírközlési vonatkozásai piaci és közigazgatáselméleti szempontból, *Jog Állam Politika,* 2022/különszám, 291–304. o.

Lattmann Tamás: Nemzetközi jogi szabályozás célzott kibertámadások esetén. In Deák Veronika (szerk.): *Célzott kibertámadások.* Budapest, Nemzeti Közszolgálati Egyetem, 2018

Lawrence Freedman: *Evolution of Nuclear Strategy.* London, Palgrave Macmillan, 2003.

Legárd Ildikó: A barát és ellenség megkülönböztetése a kibertérben. *Jog Állam Politika,* 2020/3. szám..

Lesley Kennedy: Why Reagan's ‚Star Wars' Defense Plan Remained Science Fiction. *History.* 2019 (https://www.history.com/news/reagan-star-wars-sdi-missile-defense).

Lim Min Zhang: Budget debate: SAF to set up fourth service as digital threats mount, says Ng Eng Hen. *The Straits Times.* 2022 (https://www.straitstimes.com/singapore/politics/budget-debate-saf-to-set-up-fourth-service-as-digital-threats-mount-says-ng-eng-hen).

Lina Rosenstedt: Improving Cooperation with Social Media Companies to Counter Electoral Interference. *Hybrid Coe Paper,* 2021/5. szám..

Loretta Napoleoni: *Az iszlamista főnix.* Budapest, HVG Könyvek, 2015.

Łukasz Szoszkiewicz: Internet Access as a New Human Right? State of the Art on the Threshold of 2020. *Przegląd Prawniczy Uniwersytetu Im. Adama Mickiewicza,* 2020/8. szám..

Magyary Zoltán: Két korszak mesgyéjén [mezsgyéjén]: Jogállam – a cselekvő állam. *Bányászati és Kohászati Lapok,* 1939/6. szám..

Magyary Zoltán: *Küzdelem a haladásért.* Kézirat. 1944 (http://real-ms.mtak.hu/15898/1/Ms_10640_1.pdf).

Manuel Castells: *A hálózati társadalom kialakulása. Az információ kora. Gazdaság, társadalom, kultúra. I. kötet.* Budapest, Gondolat–Infonia, 2005.

Manuel Castells: The Network Society: From Knowledge to Policy. In Manuel Castells – Gustavo Cardoso (szerk.): *The Network Society: From Knowledge to Policy.* Washington, Center for Transatlantic Relations, 2005.

Mariam Fandáková – K. Zabovska – Boris Bucko – Michal Zábovsky: Improvements of Computer Assisted Virtual Environment (CAVE). *2020 43rd International Convention on Information, Communication and Electronic Technology (MIPRO)*, 2020.

Marshall McLuhan: *A Gutenberg-galaxis.* Budapest, Trezor Kiadó, 2001.

Martin Schallbuch: Cyber-Angriffe der Bundeswehr – Eine Cyber-Armee braucht auch einen Auftrag. *Tagesspiegel Causa.* 2017. (https://causa.tagesspiegel.de/politik/darf-die-bundeswehr-cyber-attacken-zur-verteidigung-nutzen/eine-cyber-armee-braucht-auch-einen-auftrag.html).)

Márton Balázs: A NIBEK-től a Nemzeti Információs Központig, *Nemzetbiztonsági Szemle,* 2023/1. szám., 21–33. o.

Mary Aiken: *Cyber–csapda – Hogyan változtatja meg az online tér az emberi viselkedést?* Budapest, Harmat – Új Ember, 2020.

Mateus de Oliveira Fornasier: The Realization of E-Democracy in the 21st Century. *Revista da Faculdade de Direito da Universidade Federal de Minas Gerais*, 2021/jan–jun.

Matthew Andrews: *Good Government Means Different Things in Differenc Countries.* Harvard – John F. Kennedy School of Government, Faculty Research Working Papers, RWP08-068, 2008

Melvin Small – J. David Singer: The War Proneness of Democratic Regimes. *Jerusalem Journal of International Relations,* 1976/4. szám..

Merkovity Norbert: *A figyelemalapú politika a közösségi média korában. A politikai kommunikáció lehetséges értelmezése napjainkban.* Budapest, Médiatudományi Intézet, 2018.

Merle Maigre: Cyber threat actors: how to build resilience to counter them. *Hybrid CoE Paper,* 2022/11. szám..

Mezei Kitti – Szentgáli-Tóth Boldizsár: Az online platformok használatában rejlő veszélyek: a dezinformáció és a kibertámadások jogi kockázatai. In Chronowski Nóra – Szentgáli-Tóth Boldizsár – Szilágyi Emese (szerk.): *Demokrácia – Dilemmák. Alkotmányjogi elemzések a demokráciaelv értelmezéséről az Európai Unióban és Magyarországon.* Budapest, ELTE Eötvös Kiadó, 2022.

Mezei Kitti: *A kiberbűnözés aktuális kihívásai a büntetőjogban.* Budapest, TKJTI, L'Harmattan, 2020.

Mezei Kitti: *A kiberbűnözés aktuális kihívásai a büntetőjogban.* Budapest, L'Harmattan Kiadó – MTA Társadalomtudományi Kutatóközpont, Jogtudományi Intézet, 2022.

Mezei Kitti: A modern technológiák kihívásai a büntetőjogban, különös tekintettel a kiberbűnözésre. *Állam- és Jogtudomány*, 2020/4. szám..

Mezei Kitti: A szervezett bűnözés az interneten. In Mezei Kitti (szerk.): *A bűnügyi tudományok és az informatika.* Pécs, Budapest, Pécsi Tudományegyetem, MTA TK, 2019.

Mezei Kitti: Cyberterrorism – How real is the threat? In Szőke Gergely László (szerk.): *Studia Iuridica Auctoritate Universitatis Pécs Publicata. Essays of Faculty of Law University of Pécs Yearbook of 2017–2018.* Pécs, Pécsi Tudományegyetem, 2020.

Mezei Kitti: Új tendenciák a kiberbűnözés büntetőjogi megítélésében. In Gárdos Orosz Fruzsina (szerk.): *A magyar jogrendszer rezilienciája 2010 – 2020,* Budapest, ORAC Kiadó Kft., 2022, 529–549. o.

Mezey Barna – Gosztonyi Gergely (szerk.): *Magyar alkotmánytörténet.* Budapest, Osiris Kiadó, 2020.

Michael Doyle: Kant, Liberal Legacies, and Foreign Affairs. In Michael Brown – Sean Lynn-Jones – Steven E. Miller (szerk.): *Debating the Democratic Peace.* Cambridge: MIT Press, 1996.

Michael Doyle: Liberalism and World Politics. *American Political Science Review*, 1986/4. szám..

Michael Doyle: *Ways of War and Peace.* New York, Norton, 1997.

Michael Horowitz – Paul Scharre – Alex Velez-Green – A Stable: *Nuclear Future? The Impact of Automation, Autonomy, and Artificial Intelligence.* Philadelphia, University of Pennsylvania, 2017.

Michael N. Schmitt (szerk.): *Tallinn Manual 2.0 On the International Law Applicable to Cyber Operations.* Cambridge, Cambridge University Press, 2017.

Michael N. Schmitt (szerk.): *Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge, Cambridge University Press, 2013.

Michael N. Schmitt: Foreign Cyber Interference in Elections. *International Law Studies Series. US Naval War College,* 2021.

Michael Weiss – Hassan Hassan: *Az iszlám állam.* Budapest, HVG Könyvek, 2015.

Mikael Wigell – Harri Mikkola – Tapio Juntunen: *Best Practices in the Whole-of-Society Approach in Countering Hybrid Threats.* European Parliament; Directorate-General for External Policies Policy Department 2021. (Best Practices in the whole-of-society approach in countering hybrid threats (europa.eu).

Mitko Bogdanoski: Building Cyber Resilience against Hybrid Threats. *NATO Science for Peace and Security Series – D: Information and Communication Security*, 2022.

Mógor Tamás: A légierő tevékenységének jelentősége Magyarország szuverenitásának és biztonságának fenntartásában. *Hadtudomány*, 2018/6. szám..

Molnár Dóra: Nagyhatalmi kiberdiplomácia – az Egyesült Államok, Kína és Oroszország a nemzetközi kiberporondon. In Török Bernát (szerk.): *Információ- és kiberbiztonság.* Budapest, Ludovika Egyetemi Kiadó, 2020.

Molnár Ferenc: A reziliencia kérdése és a NATO. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok*, 2021/15. szám.

Muha Lajos – Krasznay Csaba: *Az elektronikus információs rendszerek biztonságának menedzselése.* Budapest, Nemzeti Közszolgálati Egyetem, 2018.

Munk Sándor: A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései. *Hadtudomány*, 2018/1. szám..

Munk Sándor: Kiberbiztonsági célok, jövőképek, szabályozók az EU-ban és kapcsolatrendszerük az interperabilitással. *Hadmérnök,* 2018/KÖFOP szám.

Muraközy László: *Az államok kora. Az európai modell.* Budapest, Akadémiai Kiadó, 2012.

Müller Tamás: Európai Uniós védelmi kezdeményezések és a PESCO. *Infojegyzet*, 2020/90. szám..

Nagy László – Tömösváry Zsigmond: *Az orosz biztonságpolitikai gondolkodás.* Budapest, Dialóg Campus Kiadó. 2018.

Nagy Zoltán – Horváth Attila (szerk.): *A különleges jogrend és nemzeti szabályozási modelljei.* Budapest, Mádl Ferenc Összehasonlító Jogi Intézet, 2021.

Nagy Zoltán András: A jövő tegnap óta tart. A modern technikai-technológiai folyamatok kihívásai a jog területén. *Belügyi Szemle*, 2018/10. szám..

Nagy Zoltán András: Kiberbűncselekmények, kiberháború, kiberterrorizmus – avagy ébresztő Magyarország! *Magyar Jog*, 2016/1. szám..

Napoleoni L.: *Modern Jihad: Tracing the Dollars Behind the Terror Networks.* London, Pluto Press, 2003.

Németh Richárd: A COVID-19 járvány okán bevezetett Home Office munkavégzés hatása a munkakörülményekre és szervezeti kommunikációra nagyvállalati környezetben. *Jog Állam Politika*, 2021/4. szám., 101. o.

Németh Richárd: A kibertérből érkező fenyegetések elleni védekezés vállalati környezetben. *GIKOF Journal*, 2021.

Németh Richárd: Kiberfenyegetettség nagyvállalati környezetben. *Magyar Bűnüldöző*, 2020/2. szám..

Németh Richárd: Kibertámadások gazdasági vonatkozásai a vállalati szférában. In Dernóczy-Polyák Adrienn (szerk.): *Kutatási jelentés 1.* Győr, Universitas-Győr Nonprofit Kft., 2019.

Neparáczki Anna Viktória: A kiberterrorizmus büntető anyagi jogi megítélése. *Ügyészek Lapja,* 2020/1. szám..

Neparáczki Anna Viktória: *A terrorizmus elleni fellépés eszközei a magyar és a német anyagi büntetőjogban.* PhD-értekezés. Pécs, 2017.

Nicholas Negroponte: *Digitális létezés.* Budapest, Typotex Kiadó, 2002.

Nicola Lucchi: Freedom of expression and the right of access to the Internet. A new fundamental right? In Monroe E. Price – Stefaan G. Verhulst – Libby Morgan: *Routledge Handbook of Media Law*, London/New York, Routledge, 2013.

Nicolas Guilhot: Automatic Leviathan: Cybernetics and politics in Carl Schmitt's postwar writings. *History of the Human Sciences*, 2020/1. szám..

Nicolas Roche: *Pourquoi la Dissuasion.* Paris, Presses Universitaires de France. 2017.

Nogel Mónika: Bűnös vagy ártatlan? Igazságügyi genetikus szakértői vélemények relevanciája a védelem számára. *Belügyi Szemle,* 2022/3. szám..

Nora Vanaga – Toms Rostoks (szerk.): *Deterring Russia in Europe.* Defence Strategies for Neighbouring States. London – New York, Routledge, 2019.

Papp Zoltán: *A légtér-szuverenitás néhány nemzetközi jogi kérdése.* Budapest, Pázmány Péter Katolikus Egyetem Jog- és Államtudományi Doktori Iskola, doktori értekezés, 2019.

Paráda István: A NATO kibervédelmi irányelveinek fejlődése. *Honvédségi Szemle*, 2018/3. szám..

Parag Khanna: *Konnektográfia. A globális civilizáció jövőjének feltérképezése.* Budapest, HVG Kiadói Zrt., 2017.

Pató Viktória Lila: *A háború hatása a közösségi médiára.* Nemzeti Közszolgálati Egyetem Európai Stratégia Kutatóintézet (https://eustrat.uni-nke.hu/hirek/2022/03/01/a-haboru-hatasa-a-kozossegi-mediara).

Patricia Wallace: *Az internet pszichológiája.* Budapest, Osiris Kiadó, 2002.

Patyi András: Good Governance and Good Public Administration. *Public Governance Andministration and Finance Law Review in the European Union and Central Eastern Europe,* 2016/1. szám..

Peschka Vilmos: *A jog sajátossága.* Budapest, Akadémiai Kiadó, 1988.

Péteri Zoltán: Az államok rendszerezése: államtípusok és államformák. In Takács Péter (szerk.): *Államelmélet. Előadások az államelmélet és az állambölcselet köréből.* Miskolc, Bíbor Kiadó, 2001.

Petruska Ferenc – Vikman László: Egy formabontó hírszerzési nyilatkozat a jogi sérülékenységek szempontjából. *Military and Intelligence CyberSecurity Research Paper,* 2021/4. szám..

Petruska Ferenc: A jogi hadviselés eszköztára. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok*, 2022/17. szám.

Petruska Ferenc: A Lawfare fogalma. *Katonai Jogi és Hadijogi Szemle*, 2021/3. szám., 97–106. o.

Petruska Ferenc: A lawfare tipológiája. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok*, 2022/16. szám..

Petruska Ferenc: Lawfare a védelmi szférában. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok*, 2022/18. szám..

Philip Bennett – Moises Naim: 21st-century censorship. *Columbia Journalism Review*, 2015/1. szám..

Philipp Lange: Total Defence. How Germany should implement a whole-of-government national and collective defence. *Security Policy Working Paper*, 2018/2. szám..

Pierre Musso: A vállalat-állam kora – avagy a politikától megfosztott politika. (Ford. Völgyes Gyöngyvér.) *Le Monde diplomatique – magyar kiadás*, 2019. július.

Piotr Szymanski: *New Ideas for Total Defence. Comprehensive Security in Finland and Estonia.* Warsaw, Centre for Eastern Studies, 2020.

Piret Pernik (szerk.): *Cyberspace Strategic Outlook 2030.* Tallinn, CCDCOE, 2022.

Pócza Kálmán: *Álmaink állama. Egy hatalmi centrum az ezredfordulón.* Budapest, Századvég Kiadó, 2002.

Pongrácz Alex – Téglási András: Szociális állam, jóléti állam – Elméleti és történeti alapvetés. In Bódi Stefánia – Schweitzer Gábor (szerk.): *Az emberi jogok alkotmányos védelme Magyarországon.* Budapest, Ludovika Egyetemi Kiadó, 2021.

Pongrácz Alex: A közmenedzsment-reformok metamorfózisai. *Új Magyar Közigazgatás*, 2016/1. szám., 1–12. o.

Pongrácz Alex: A politika folytatása más eszközökkel? Avagy gondolatok az állam és az erőszak kérdésköréről. *Államtudományi Műhelytanulmányok*, 2017/17. szám..

Pongrácz Alex: Az állam gazdaságpolitikai szerepvállalásának változásai. *Pro Publico Bono*, 2017/3. szám..

Pongrácz Alex: Mozaikok a magyar szuverenitásfelfogás történetéből. In Karácsony András (szerk.): *Szuverenitáskérdések. Elméletek, történetek.* Budapest, Gondolat Kiadó, 2020.

Pongrácz Alex: *Nemzetállamok és új szabályozó hatalmak a globális erőtérben – avagy megszelídíthető-e a globalizáció?* Budapest, Dialóg Campus, 2019.

Pongrácz Alex: Szuverenitás és alkotmányosság a globális erőtérben. *Pro Publico Bono,* 2016/1. szám..

Porkoláb Imre – Hennel Sándor – Hegedűs Ernő: Modernizáció és innováció (1.). *Honvédségi Szemle*, 2021/2. szám., 14–26. o.

Póti László: Minszk–2 után két évvel: Hol tart a békefolyamat? *KKI Elemzések*, 2017/5. szám..

Pölöskei János: A képességalapú haderőtervezés. *Honvédségi Szemle*, 2021/6. szám..

Quareshi Waseem Ahmad: Information Warfare, International Law, and the Changing Battlefield. *Forsham International Law Journal,* 2020/4. szám..

Rab Judit – Szemerey Samu: *Az okos város fejlesztési modell módszertani alapjai.* Budapest, Lechner Nonprofit Kft., 2018.

Rácz Lilla: A személy és a dolog fogalmának (lehetséges) változásai a mesterséges intelligencia és a kriptovaluták világában. *Állam- és Jogtudomány*, 2020/4. szám..

Rada Péter: Átalakuló biztonsági kihívások. A biztonság dimenziói. *Grotius*, 2007 (Rada P\351ter \301talakul\363 biztons\341gpolitikai kih\355v\341sok.doc) (grotius.hu).

Rainer Hermann: *Az iszlám állam.* Budapest, Akadémiai Kiadó, 2015

Ray Kurzweil: *A szingularitás küszöbén.* Budapest, Ad Astra, 2014.

Resperger István: Stratégiák és fogalmak háborúja, az aszimmetrikus hadviselés hadtudományi megközelítése. *Hadtudomány,* 2016/Elektronikus szám.

Richard Cobden: *Political Writings of Richard Cobden.* London Ridgway, 1901.

Richard Sussking: *Online Courts and the Future of Justice.* Oxford, Oxford University Press, 2019.

Richard Titmuss: Universal versus Selection. In Christopher Piersen – Francis G. Castel (szerk.): *The Welfare State Reader.* (Second Edition.) Cambridge, Polity Press, 2006.

Rixer Ádám (szerk.): *A járvány hosszútávú hatása a magyar közigazgatásra.* Budapest, Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar Lőrincz Lajos Közjogi Kutatóműhely, 2021.

Robert Post: Participatory Democracy and Free Speech. *Virginia Law Review*, 2011/3. szám..

Ronkovics József: A 21. század hadviselésének néhány főbb jellemzője. *Hadtudomány,* 2009/1–2. szám.

Rostoványi Zsolt: Civilizációk a civilizáció ellen? A hidegháború utáni nemzetközi rendszer antinómiái. *Külügyi Szemle*, 2002/1. szám..

Rostoványi Zsolt: Terrorizmus és szabadság. *Fundamentum,* 2001/4. szám..

Sajó András: *A szólásszabadság kézikönyve.* Budapest, KJK-Kerszöv, 2005.

Samuel P. Huntington: *A civilizációk összecsapása és a világrend átalakulása.* Budapest, Európa Könyvkiadó, 2006.

Sascha Dov Bachmann – Andres B. Munoz Mosquera: Lawfare and hybrid warfare – how Russia is using the law as a weapon. Amicus Curiae. *Journal of the Society for Advanced Legal Studies*, Summer 2015, 25–28. o.

Sascha-Dominik Bachmann – Hakan Gunneriusson: Hybrid Wars: The 21st Century's New Threats to Global Peace and Security. *South African Journal of Military Studies*, 2015/1. szám..

Schubert Bálint: Az autonóm fegyverrendszerekkel szemben támasztott követelmények a humanitárius nemzetközi jog tükrében. *Honvédségi Szemle,* 2022/3. szám..

Scott Carpenter: The Internet Shutdowns Issue. *The Current*, 2021/4. szám. (https://jigsaw.google.com/the-current/shutdown/).

Scott D. Applegate: The Dawn of Kinetic Cyber. In K. Podins – J. Stinissen – M. Maybaum (szerk.): *2013 5th International Conference on Cyber Conflict Proceedings.* Tallinn, NATO CCD COE Publications, 2013.

Scott N. Romaniuk – Mary Manjikian (szerk.): *Routledge Companion to Global Cyber-Security Strategy.* New York, Routledge, 2021.

Sean S. Costigan – David Gold: *Terronomics ASHGATE.* Printed in Great Britain, 2007.
Selján Péter: A közel-keleti hatalmi egyensúly átalakulása. *Nemzet és Biztonság – Biztonságpolitikai Szemle*, 2016/4. szám..
Sepsi Tibor: *GDPR útikalauz adatkezelőknek.* Budapest, Wolters Kluwer, 2019.
Serbakov Márton Tibor: *Egyes szélsőséges terrorista csoportok internethasználata egyes aspektusainak elemzése.* PhD-értekezés. Pécs, Pécsi Tudományegyetem, 2022
Sieber–Vogel: *Terrorismusfinanzierung: Prävention im Spannungsfeld von internationalen Vorgaben und nationalem Tatstrafrecht.* Berlin, Duncker & Humblot, 2015.
Simicskó István: A terrorizmus elleni védelem fokozása a különleges jogrendi kategóriák bővítésével. *Hadtudomány*, 2016/3–4. szám., 100–113. o.
Simon A. Herbert: *Korlátozott racionalitás.* Budapest, Közgazdasági és Jogi Könyvkiadó, 1982.
Simon László – Magyar Sándor: A terrorizmus és indirekt hadviselése az EU kiberterében. *Szakmai Szemle*, 2017/4. szám..
Simon László – Magyar Sándor: A terrorizmus és indirekt hatása a kiberterében. *Szakmai Szemle*, 2017/3. szám..
Simon László: A fokozódó terrorizmus Európában és annak hatása a katonai tömegrendezvények biztosítására. *Szakmai Szemle,* 2015/2. szám..
Simon László: A partizán elmélete a premodern virtuális korban: A partizán elmélete az információs környezet speciális műveleteiben. *Jog Állam Politika*, 2017/4. szám..
Simon László: A válságkezelés során felhasználható nemzetbiztonsági információk katonai oldala. In Orbók-Barkovics Veronika – Orbók Ákos: *A hadtudomány és a XXI. század 2018.* Budapest, DOSZ Hadtudományi Osztály, 2018, 251. o.
Simon László: Az információ mint fegyver? *Szakmai Szemle*, 2016/1. szám..
Siposné Kecskeméthy Klára: A NATO 2030 jelentés – stratégiai prioritások új megközelítésben. *Honvédségi Szemle*, 2021/4. szám..
Sipri Yearbook 2022 – Armaments, Disarmament and International Security (https://www.sipri.org/yearbook/2022).
Somkutas Péter – Kőhidi Ákos: Az önvezető autó szoftvere magas szintű szellemi alkotás vagy kifinomult károkozó? *In Media Res*, 2017/2. szám..
Spitzer Jenő: A francia kibervédelmi és kiberbiztonsági rendszer egyes stratégiai aspektusai. *Military and Intelligence CyberSecurity Research Paper*, 2021/3. szám..
Spitzer Jenő: *Önvédelem versus terrorizmus. Az erőszak tilalma és az önvédelem joga a nemzetközi jogban, különös tekintettel az Iszlám Állam elleni nemzetközi fellépés lehetőségeire.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2019.
Stefan Heumann: Cyberkrieg und die Bundeswehr – Warum Cyber-Gegenangriffe gefährlich sind. *Tagespiegel Causa.* 2017 (https://causa.tagesspiegel.de/politik/darf-die-bundeswehr-cyber-attacken-zur-verteidigung-nutzen/warum-cyber-gegenangriffe-gefaehrlich-sind.html).
Stephen Van Evera: Primed for Peace. *International Security*, 1990/1. szám..
Steve Chan: Mirror, Mirror on the Wall… Are the Freer Countries More Pacific. *Journal of Conflict Resolution*, 1984/4. szám..
Steven Koetler: *A lehetetlen művészete.* Budapest, HVG Könyvek Kiadó, 2021.

Steven Mark Levy: *Federal Money Laundering Regulation (Banking, Corporate, and Securities Compliance)*. New York, 2003.

Stuart Russell – Peter Norvig: *Artificial Intelligence: A Modern Approach*. Harlow, Pearson Education, 2014.

Stumpf István (szerk.): *Erős állam – alkotmányos korlátok*. Budapest, Századvég Kiadó, 2014.

Stumpf István: A „jó kormányzás" két értelme. Avagy a demokratikus kormányzás programja és feltételei. In Stumpf István (szerk.): *Erős állam, alkotmányos korlátok*. Budapest, Századvég Kiadó, 2014.

Stumpf István: A jó kormányzás felé. In Stumpf István (szerk.): *Erős állam, alkotmányos korlátok*. Budapest, Századvég Kiadó, 2014.

Stumpf István: Neoweberi állam és jó kormányzás. Avagy mit tennél, ha te volnál az állam? In Stumpf István: *Erős állam, alkotmányos korlátok*. Budapest, Századvég Kiadó, 2014.

Stumpf István: Új államalapítás? Alkotmányos és kormányzati kihívások. In Stumpf István (szerk.): *Erős állam – alkotmányos korlátok*. Budapest, Századvég Kiadó.

Sulyok Gábor: A terrorcselekmény elkövetéséhez használt polgári légi jármű lelövésének alkotmányjogi megítélése az új szabályozási környezetben. In Bartkó Róbert (szerk.): *A terrorizmus elleni küzdelem aktuális kérdései a 21. században*. Budapest, Gondolat Kiadó, 2019.

Sven Lilienström: Jeder kann einen Cyber-Angriff für weniger als 18 Euro beauftragen. *The European*. 2020 (https://www.theeuropean.de/sven-lilienstroem/cybersicherheit-in-deutschland/).

Szabadfalvi József: Jogállam – cselekvő állam: Magyary Zoltán jogállam-felfogásának rekonstrukciója. *Pro Futuro*, 2022/1. szám..

Szádeczky Tamás: Terrorizmus a kibertérben. *Infokommunikáció és Jog*, 2008/5. szám..

Szalai Ádám: Az okosváros-koncepciók kritikai földrajzi vizsgálata – elméleti háttér és lehetséges kutatási irányok. *Tér és Társadalom*, 2020/2. szám..

Szenes Zoltán: Katonai biztonság napjainkban. Új fenyegetések, új háborúk, új elméletek. In Finiszter Géza – Sabjanics István (szerk): *Biztonsági kihívások a 21. században*. Budapest, Dialog Campus, 2017.

Szentgáli Gergely: A NATO kibervédelmi politikájának fejlődése. *Bolyai Szemle*, 2012/2. szám..

Szentgáli Gergely: Csendben szolgálni: 1. rész: A magyar nemzetbiztonsági szektor helyzete és átalakítása 2010 és 2014 között. *Hadtudomány*, 2015/1–2. szám..

Szentgáli Gergely: The NATO Policy on Cyber Defence: The Road so Far. *AARMS*, 2013/1. szám..

Szépvölgyi Enikő: A dualizmuskori állami gyermekvédelem és a szegényügy összefüggései. *Jog Állam Politika*, 2020/3. szám..

Szépvölgyi Enikő: Gondolatok az állami gyermekvédelemről szóló törvénycikkek 120. évfordulójára. In Mezey Barna (szerk.): *Kölcsönhatások. Európa és Magyarország a jogtörténelem sodrásában*. Budapest, Gondolat Kiadó, 2021.

Szigeti Péter: Az állam mozgáspályájának átfogó íve és csomópontjai a jelenkorban. In Egresi Katalin et al.: *Államelmélet*. Győr, Széchenyi István Egyetem Deák Ferenc Állam- és Jogtudományi Kar Jogelméleti Tanszék, 2016.

Szigeti Péter: Kapitalizmus és a tőkés termelési mód elmélete. *Eszmélet*, 2019.

Szigeti Péter: *Társadalomkutatás – Mi végre? Politikatudomány, alkotmányjog, világrendszer-elmélet*, Győr, Universitas, 2011.

Szigeti Péter: Vázlat a közbiztonság három dimenziójáról: világrendszer – nemzetállami szint és lokalitás. In Szigeti Péter: *A valóság vonzásában – Jogelméleti* és *Jogtudományi Közlöny*, Győr, ELTE–SZIF ÁJK, 2001 (https://mek.oszk.hu/04200/04241/04241.htm#16).

Szikszai Marcel: Disztópia Kínában? Tanulmány a társadalmi kreditrendszer a kínai jogfejlődés tükrében. *Infokommunikáció és Jog*, 2020/1. szám..

Szkála Károly – Munk Sándor: A kibertér fogalma, értelmezése és fejlődése. *Földrajzi Közlemények*, 2018/4. szám..

Szövényi György: A terrorizmus jellegzetességei az ezredfordulón. *Európai Tükör*, 1998/3. szám..

Szűrös Éva et al. (szerk.): *„A cselekvés állama". Dr. Kiss István emlékkötet.* Budapest, Agroinform Kiadó, 2006.

Takács Péter: *Államtan. A modern állam és elmélete. Két fejezet az állam általános elmélete köréből.* Budapest, Nemzeti Közszolgálati Egyetem, 2012.

Takács Péter: Észrevételek az államforma fogalmához. *Jog – Állam – Politika.* Ünnepi különszám Kukorelli István tiszteletére. 2022/2. különszám.

Tálas Péter: A vasói NATO-csúcs legfontosabb döntéseiről. *Nemzet és Biztonság*, 2016/2. szám..

Tálas Péter: Tatárszentgyörgy után… – A biztonság szubjektív percepciójának veszélyeiről. *Nemzet és Biztonság*, 2009/február.

Tanyi Lakhtakia – Ameya Bondre – John Torous at. al.: Smartphone digital phenotyping, surveys, and cognitive assessments for global mental health: Initial data and clinical correlations from an international first episode psychosis study. *Digital Health*, 2022/november (https://journals.sagepub.com/doi/10.1177/20552076221133758).

Tawia Ansah: Lawfare: A Rhetorical Analysis. *Case Western Reserve Journal of International Law*, 2010, 87–119. o.

Tero–SæbØ Øystein Päivärinta: Models of E-Democracy. In *Communications of the Association for Information Systems,* 2006/1. szám..

Thomas E. Kadri: Digital Gatekeepers. *Texas Law Review*, 2021/5. szám.

Thomas Hobbes: *Leviatan I–II.* Budapest, Kossuth Kiadó, 1999.

Thomas J. Bierstecker – Sue E. Eckert (szerk.): *Countering th Financing of Terrorism.* London, New York, 2008.

Tiina Ferm: *Laws in the Era of Hybrid Threats.* Helsinki, The European Centre of Excellence for Countering Hybrid Threats, 2017

Tilesch György – Omar Hatamleh: *Mesterséges intelligencia – Vegyük kezünkbe a sorsunkat az MI korában.* Budapest, Libri, 2021.

Timár Adrienn: Digitális szerzői jog. In Sajtiné Sándor Erika (szerk.): *Bevezetés a szerzői jogba.* Budapest, Szellemi Tulajdon Nemzeti Hivatala, 2020, 40–44. o.; Ződi Zsolt: Az európai platformszabályozás jellegezetességei. *In Medias Res* 2022/1. szám., 66–82. o.

Tom Abate: Smarter Hospitals: How AI-Enabled Sensors Could Save Live. *HAI Stanford University Human-Center Artificial Inteligence,* 2020. 09. 09. (https://hai.stanford.edu/news/smarter-hospitals-how-ai-enabled-sensors-could-save-lives).

Tom Christensen – Per Lægreid: The Whole-of-Government Approach to Public Sector Reform. *Stein Rokkan Centre for Social Studies – Working Paper*, 2006/6. szám..

Tölgyesi Beatrix: Az orosz „szuverén internet" törvényről. *Nemzet és Biztonság: Biztonságpolitikai Szemle*, 2020/2. szám..

Török Bernát – Ződi Zsolt (szerk.): *Az internetes platformok kora,* Budapest, Ludovika Egyetemi Kiadó, 2022.

Trivedi, Upmanyu: India Court Finds Indefinite Restrictions in Kashmir Illegal. *Bloomberg*, 2020. január 10. (https://www.bloomberg.com/news/articles/2020-01-10/top-court-rules-limitless-internet-shutdown-in-kashmir-illegal).

Ugrin Emese – Varga Csaba: *Új állam- és demokráciaelmélet.* Budapest, Századvég Kiadó, 2007.

Urbán Attila: A koordinációs folyamatok intézményi hátterének evolúciója a magyar nemzetbiztonsági igazgatásban. *Nemzetbiztonsági Szemle*, 2020/1. szám..

Urbán Attila: A koordinációs folyamatok intézményi hátterének evolúciója a magyar nemzetbiztonsági igazgatásban, *Nemzetbiztonsági Szemle,* 2020/1. szám., 5–32. o.

Vajda János Álmodnak-e az androidok elfogult bírókkal? Kognitív torzítások és önbeteljesítő jóslatok a mesterséges intelligencia peres előrejelzéseiben. *Infokommunikáció és Jog,* 2022/1. szám..

Varga Csaba: Az állam és a közigazgatás új elmélete. *Polgári Szemle*, 2006/2–3. szám..

Vaszari Tamás: *Oroszország geogazdasági és geopolitikai dilemmái a XXI. század elején, valamint ezek történelmi előzményei.* Győr. Széchenyi István Egyetem. Doktori értekezés, 2018.

Végh Károly: Információs és befolyásolási műveletek a nemzetközi jog „szürke zónájában". In Farkas Ádám – Végh Károly (szerk.): *Új típusú hadviselés a 21. század második évtizedében és azon túl. Intézményi és jogi kihívások.* Budapest, Zrínyi Kiadó, 2020.

Vikman László: A közműszolgáltatások és a reziliencia egyes kérdései, különös tekintettel a kiberbiztonságra, *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok*, 2021/14. szám..

Vikman László: A műveletszervezés jogi feladatai. *Honvédségi Szemle*, 2021/2. szám..

Vikman László: A német kiberbiztonsági szisztéma áttekintése. Szervezeti keretek, különös tekintettel a nemzetbiztonsági szolgálatok és a hadsereg szerepére és kapcsolatára, valamint a szabályozási háttér alakulására. *Military and Intelligence CyberSecurity Research Paper*, 2021/2. szám..

Vikman László: Gondolatok a kiberbiztonsági stratégiák fejlesztésére vonatkozó nemzetközi útmutató kapcsán. *SmartLaw Research Group Workin Paper*, 2022/1. szám..

Vincent Boulanin (szerk.): *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk, vol. I, Euro-Atlantic Perspectives.* Stockholm, SIPRI Publications, 2019.

Vincent Lamigeon: Budget des Armées 2019: Qui Sont les Gagnants? *Challenges*, 2018.

Vincent Mosco: *Okosvárosok a digitális világban.* Budapest, Pallas Athéné Könyvkiadó, 2019.

William E. Leigher: Cyber conflict in a hybrid threat environment: Death by a thousand cuts. *Hybrid CoE Paper*, 2021/10. szám..

William Temple: *Citizen and Churchman.* London, Eyre & Spottiswoode Publishers, 1941.

Wolf-Diether Roepke – Hasit Thankey: Resilience The First Line Of Defence. *The Three Swords Magazine*, 2019/34. szám..

Yuval Noah Harari: *Homo Deus. – A holnap rövid története.* Budapest, Animus Kiadó, 2016.
Yvonne Hofstetter: *Láthatatlan háború, avagy miképpen fenyegeti a digitalizáció a világ biztonságát és stabilitását.* Budapest, Corvina, 2020.
Z. Karvalics László: Marshall McLuhan helye az információs társadalom elmélettörténetében. *Replika,* 2011/3. szám..
Zygmunt Bauman: *Globalizáció.* Szeged, Szukits Könyvkiadó, 2002.
Zsidai Ágnes: Legitimitás és legitimáció. In Takács Péter (szerk.): *Államelmélet.* Miskolc, Bíbor, 1997.